

JP2002288448 A

LICENSE RECORDER

SANYO ELECTRIC CO LTD

Inventor(s):HORI YOSHIHIRO ;YOSHIKAWA TAKATOSHI

Application No. 2001087395 JP2001087395 JP, Filed 20010326,A1

Published 20021004Published 20021004

Abstract:

PROBLEM TO BE SOLVED: To provide a license recorder which provides a backup of a leased license.

SOLUTION: A memory card 1 is provided with a license area 1415A. The license area 1415A includes licenses (a license ID, a contents ID, a license key Kc, access control information Acn, and reproducing frequency control information Acp), a validity flag, a lease flag, a leased party ID, and license ID at the time of lease. When the license is leased 'under lease' is set to the lease flag, and a public cipher key peculiar to a memory card of the leased party is stored in the leased party ID, and the license ID for lease is stored in the license ID at the time of lease.

Int'l Class: G06F01760; G06K01700 G06K01907

Patents Citing this One: No US, EP, or WO patents/search reports have cited this patent. MicroPatent Reference Number: 000647412

COPYRIGHT: (C) 2002JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-288448

(P2002-288448A)

(43) 公開日 平成14年10月4日 (2002.10.4)

| (51) Int.Cl. <sup>7</sup> | 識別記号                             | F I           | テーマコード*(参考)  |
|---------------------------|----------------------------------|---------------|--|
| G 0 6 F 17/60             | 3 0 2<br>Z E C<br>1 4 2<br>5 0 2 | G 0 6 F 17/60 | 3 0 2 E 5 B 0 3 5<br>Z E C 5 B 0 5 8<br>1 4 2<br>5 0 2 |
| G 0 6 K 17/00             |                                  | G 0 6 K 17/00 | L  |

審査請求 未請求 請求項の数 9 O L (全 44 頁) 最終頁に続く

(21) 出願番号 特願2001-87395(P2001-87395)

(22) 出願日 平成13年3月26日 (2001.3.26)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 堀 吉宏

大阪府守口市京阪本通2丁目5番5号 三  
洋電機株式会社内

(72) 発明者 吉川 隆敏

大阪府守口市京阪本通2丁目5番5号 三  
洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

Fターム(参考) 5B035 AA13 BB09 BC00 CA38

5B058 CA27 KA02 KA04 KA08 KA35

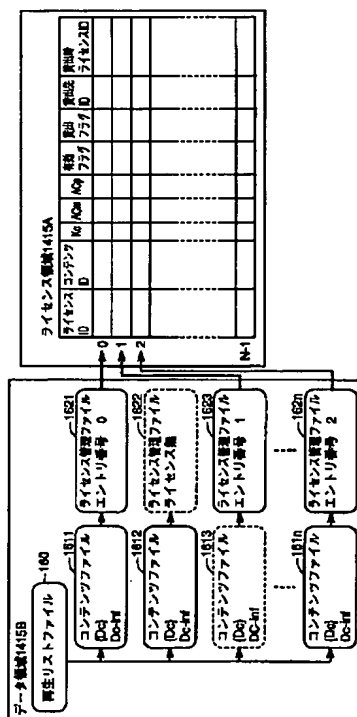
YA20

(54) 【発明の名称】 ライセンス記録装置

(57) 【要約】

【課題】 貸出したライセンスのバックアップを提供できるライセンス記録装置を提供する。

【解決手段】 メモリカードは、ライセンス領域1415Aを備える。ライセンス領域1415Aは、ライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、および再生回数制御情報ACp)、有効フラグ、貸出フラグ、貸出先ID、および貸出時ライセンスIDを含む。ライセンスの貸出が行なわれると、貸出フラグに「貸出中」が設定され、貸出先IDに貸出先のメモリカードに固有な公開暗号鍵が格納され、貸出時ライセンスIDに貸出用ライセンスIDが格納される。



## 【特許請求の範囲】

【請求項 1】 暗号化コンテンツデータを復号するためのライセンスから貸出用ライセンスを生成し、前記貸出用ライセンスを他のライセンス記録装置へ貸出すライセンス記録装置であって、

前記ライセンスと、前記ライセンスの貸出可否を示す貸出フラグと、前記貸出用ライセンスの貸出先を特定するための貸出先特定情報と、前記貸出用ライセンスを識別するための貸出用ライセンス識別情報とを保持するライセンス保持部と、制御部とを備え、

前記制御部は、前記ライセンスの貸出要求に応じて、前記他のライセンス記録装置への貸出の対象となるライセンスを指定するためのライセンス指定情報と前記貸出用ライセンスを特定するための貸出用ライセンス特定情報とを外部から受け、前記ライセンス指定情報によって指定されたライセンスを前記ライセンス保持部から読出し、その読出したライセンスに含まれ、かつ、前記読出したライセンスを特定するためのライセンス特定情報を前記貸出用ライセンス特定情報に代えて前記貸出用ライセンスを生成し、前記貸出フラグを貸出中に設定する、ライセンス記録装置。

【請求項 2】 前記制御部は、前記ライセンス保持部から読出したライセンスが、複製を禁止され、かつ、移動が許可されたライセンスであるとき、前記貸出用ライセンスを生成する、請求項 1 に記載のライセンス記録装置。

【請求項 3】 前記制御部は、前記貸出フラグが前記ライセンスを貸出していないことを示すとき、前記貸出用ライセンスを生成する、請求項 1 または請求項 2 に記載のライセンス記録装置。

【請求項 4】 前記制御部は、さらに、前記他のライセンス記録装置における前記貸出用ライセンスの移動および複製を禁止するための制御情報を生成し、前記ライセンス保持部から読出したライセンスに含まれ、かつ、前記読出したライセンスの複製を禁止した制御情報を、前記生成した制御情報に代えて前記貸出用ライセンスを生成する、請求項 1 から請求項 3 のいずれか 1 項に記載のライセンス記録装置。

【請求項 5】 前記制御部は、さらに、前記貸出用ライセンス特定情報を前記貸出用ライセンス識別情報として前記ライセンス保持部に格納する、請求項 1 から請求項 4 のいずれか 1 項に記載のライセンス記録装置。

【請求項 6】 前記制御部は、さらに、前記他のライセンス記録装置に固有な公開暗号鍵を前記他のライセンス記録装置から受信し、その受信した公開暗号鍵を前記貸出先特定情報として前記ライセンス保持部に格納する、請求項 1 から請求項 5 のいずれか 1 項に記載のライセンス記録装置。

【請求項 7】 前記ライセンス保持部は、領域を指定す

るエントリ番号に対応して前記ライセンス、前記貸出フラグ、前記貸出先特定情報、および前記貸出用ライセンス識別情報を格納しており、

前記制御部は、前記ライセンス指定情報として前記エントリ番号を外部から受ける、請求項 1 から請求項 6 のいずれか 1 項に記載のライセンス記録装置。

【請求項 8】 前記ライセンス保持部は、前記貸出先特定情報と前記貸出用ライセンス識別情報とをライセンスの貸出先の数に応じて保持する、請求項 1 から請求項 7 のいずれか 1 項に記載のライセンス記録装置。

【請求項 9】 前記ライセンスによって再生される暗号化コンテンツデータを記録するデータ格納部をさらに備える、請求項 1 から請求項 8 のいずれか 1 項に記載のライセンス記録装置。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを他のライセンス記録装置へ貸出すライセンス記録装置に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易に情報通信網にアクセスし、情報通信網上のデータを取得することが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の作者の創作物であるコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大する情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のような情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録した CD（コンパクトディスク）については、CD から光磁気ディスク（MD 等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体

やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データを情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信すること

も行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータの配信においては、パーソナルコンピュータにインストールされたソフトウェアによって暗号化コンテンツデータの配信が行なわれており、暗号化コンテンツデータに対するセキュリティは、暗号化コンテンツデータをメモリカードに書込む場合より低い。また、上記のメモリカードと同じセキュリティを持つデバイスをパーソナルコンピュータに装着すれば、上記の携帯電話機に対する暗号化コンテンツデータの配信と同じ配信をパーソナルコンピュータに対して行なうことが可能である。

【0015】そうすると、パーソナルコンピュータは、インストールされたソフトウェアと、上記デバイスとによって暗号化コンテンツデータを受信する。つまり、パーソナルコンピュータは、セキュリティレベルの異なる暗号化コンテンツデータを受信する。

【0016】さらに、音楽データが記録された音楽CDが広く普及しており、この音楽CDから音楽データをリッピングによって取得することも行なわれている。そして、このリッピングによって音楽データから暗号化音楽データ（暗号化コンテンツデータ）と、その暗号化音楽データを復号して再生するためのライセンスとが生成される。そして、このリッピングにおいては、コンテンツデータの利用規則を規定するウォーターマークをコンテンツデータから検出し、その検出したウォーターマークの内容に応じて暗号化コンテンツデータおよびライセンスが生成される。

【0017】上述したように、携帯電話機およびパーソナルコンピュータは、配信サーバから暗号化された暗号化コンテンツデータおよびライセンスを受信する。そして、携帯電話機およびパーソナルコンピュータのユーザは、受信した暗号化コンテンツデータおよびライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ移動または複製することもある。この場合、ユーザは、暗号化コンテンツデータを他のユーザの携帯電話機またはパーソナルコンピュータへ移動／複製することは自由であるが、暗号化コンテンツデータを復号するライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ自由に移動することはできない。つまり、ライセンスは、コンテンツ供給者の定めた条件に従って制御され、複製が自由に行なえるライセンス、複製を禁止するものの移動を許可するライセンス、複製・移動とともに禁止するライセンスが存在する。また、音楽CDからのリッピングでは、通常、著作権保護の観点から複製も移動も禁止しておく必要がある。他のユーザの携帯電話機またはパーソナルコンピュータへ移動したとき、暗号化コンテンツデータの著作権保護の観点から送信側と受信側との両方にライセンスを残すことはできない。そこで、ライセンスの移動を行なったとき、送信側のライセンスを消去する。

【0018】また、移動および複製が禁止されたライセンスに対しては、返却を条件として他のメモリカード等へライセンスを貸出すことが行なわれている。

【0019】

【発明が解決しようとする課題】しかし、従来のライセンスの貸出においては、貸出したライセンスと貸出元にあるライセンスとを1対1に対応付けて、貸出元において管理することができない。つまり、貸出元において、貸出したライセンスのバックアップを提供することができないという問題があった。

【0020】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、貸出したライセンスのバックアップを提供できるライセンス記録装置を提供することである。

【0021】

【課題を解決するための手段】この発明によれば、ライセンス記録装置は、暗号化コンテンツデータを復号するためのライセンスから貸出用ライセンスを生成し、貸出用ライセンスを他のライセンス記録装置へ貸出すライセンス記録装置であって、ライセンスと、ライセンスの貸出可否を示す貸出フラグと、貸出用ライセンスの貸出先を特定するための貸出先特定情報と、貸出用ライセンスを識別するための貸出用ライセンス識別情報とを保持するライセンス保持部と、制御部とを備え、制御部は、ライセンスの貸出要求に応じて、他のライセンス記録装置への貸出の対象となるライセンスを指定するためのライセンス指定情報と貸出用ライセンスを特定するための貸出用ライセンス特定情報とを外部から受け、ライセンス指定情報によって指定されたライセンスをライセンス保持部から読出し、その読出したライセンスに含まれ、かつ、読出したライセンスを特定するためのライセンス特定情報を貸出用ライセンス特定情報に代えて貸出用ライセンスを生成し、貸出フラグを貸出中に設定する。

【0022】好ましくは、制御部は、ライセンス保持部から読出したライセンスが、複製を禁止され、かつ、移動が許可されたライセンスであるとき、貸出用ライセンスを生成する。

【0023】好ましくは、制御部は、貸出フラグがライセンスを貸出していないことを示すとき、貸出用ライセンスを生成する。

【0024】好ましくは、制御部は、さらに、他のライセンス記録装置における貸出用ライセンスの移動および複製を禁止するための制御情報を生成し、ライセンス保持部から読出したライセンスに含まれ、かつ、読出したライセンスの複製を禁止した制御情報を、生成した制御情報に代えて貸出用ライセンスを生成する。

【0025】好ましくは、制御部は、さらに、貸出用ライセンス特定情報を貸出用ライセンス識別情報としてライセンス保持部に格納する。

【0026】好ましくは、制御部は、さらに、他のライ

センス記録装置に固有な公開暗号鍵を他のライセンス記録装置から受信し、その受信した公開暗号鍵を貸出先特定情報としてライセンス保持部に格納する。

【0027】好ましくは、ライセンス保持部は、領域を指定するエントリ番号に対応してライセンス、貸出フラグ、貸出先特定情報、および貸出用ライセンス識別情報を格納しており、制御部は、ライセンス指定情報としてエントリ番号を外部から受ける。

【0028】好ましくは、ライセンス保持部は、貸出先特定情報と貸出用ライセンス識別情報とをライセンスの貸出先の数に応じて保持する。

【0029】好ましくは、ライセンス記録装置は、ライセンスによって再生される暗号化コンテンツデータを記録するデータ格納部をさらに備える。

【0030】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0031】図1は、本発明によるライセンス記録装置が暗号化コンテンツデータを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0032】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話に装着されたメモリカード110に、またはインターネットを介してデジタル音楽データを各パーソナルコンピュータに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても適用することが可能なものである。

【0033】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、ユーザからの配信要求

(配信リクエスト)を配信サーバ10に中継する。著作権の存在する音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ(以下コンテンツデータとも呼ぶ)を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【0034】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

【0035】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0036】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0037】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ10からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0038】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0039】また、図1においては、パーソナルコンピュータ50は、メモリカード110のライセンス管理に関わる機能と同一機能を備えたライセンス管理デバイス（ハードウェア）を備えることで、携帯電話機100およびメモリカード110を用いて受信したのと同じセキュリティレベルの配信を受けることができる。そして、パーソナルコンピュータ50は、インターネット網30を介して、暗号化コンテンツデータとライセンスとを配信サーバ10から受信する。このとき、ライセンスは、配信サーバ10とライセンス管理デバイスとの間で所定の手順に従った暗号通信路を用いて、直接、ライセンス管理デバイスにおいて受信され、記録される。暗号化コンテンツデータはそのままHDDに記録される。このライセンス管理デバイスは、メモリカード110と同じようにライセンスの送受信や管理の機密性をハード的に保持するものであり、機密性が高いものである。

【0040】さらに、図1においては、パーソナルコンピュータ50は、ライセンス管理モジュールを使って音楽データを記録した音楽CD（Compact Disk）60から取得した音楽データからローカル使用に限定された暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを生成する。この処理をリッピングと呼び、音楽CDから暗号化コンテンツデータとライセンスとを取得する行為に相当する。リッピングの詳細については後述する。

【0041】またさらに、パーソナルコンピュータ50は、USB（Universal Serial Bus）ケーブル70によって携帯電話機100と接続さ

れ、暗号化コンテンツデータおよびライセンスを携帯電話機100に装着されたメモリカード110と送受信することが可能である。

【0042】更に、図1においては、パーソナルコンピュータ50は、ハードウェアによって機密性を持つコンテンツ再生回路をパーソナルコンピュータに備えれば暗号化コンテンツデータの再生が可能となる。また、ソフトウェアによるコンテンツ再生であっても、十分な機密性が確保できれば、再生可能となる。パーソナルコンピュータにおける再生についての詳細な説明は、本出願における説明を簡略化するために省略する。

【0043】したがって、図1に示すデータ配信システムにおいては、パーソナルコンピュータ50は、インターネット網30を介して配信サーバ10から暗号化コンテンツデータとライセンスとを受信するとともに、音楽CDから暗号化コンテンツデータとライセンスとを取得する。また、携帯電話機100に装着されたメモリカード110は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータおよびライセンスを受信するとともに、パーソナルコンピュータ50が配信サーバ10または音楽CD60から取得した暗号化コンテンツデータおよびライセンスを受信する。携帯電話機100のユーザは、パーソナルコンピュータ50を介することによって音楽CDから暗号化コンテンツデータおよびライセンスを取得することが可能となる。

【0044】さらに、携帯電話機100に装着されたメモリカード110は、携帯電話網を介して配信サーバ10から受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ50に待避することが可能となる。

【0045】図2は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータおよびライセンスを受信する機能を有しない再生端末102を用いた場合のデータ配信システムを示したものである。図2に示すデータ配信システムにおいては、再生端末102に装着されたメモリカード110は、パーソナルコンピュータ50が配信サーバ10または音楽CD60から取得した暗号化コンテンツデータおよびライセンスを受信する。このように、パーソナルコンピュータ50が暗号化コンテンツデータおよびライセンスを取得することによって通信機能のない再生端末102のユーザも暗号化コンテンツデータを受信することができるようになる。

【0046】図1および図2に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話またはパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するため

のコンテンツデータ保護を実現する構成である。

【0047】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機またはパーソナルコンピュータとも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0048】なお、以下の説明においては、配信サーバ10から、各携帯電話機、各パーソナルコンピュータ等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0049】図3は、図1および図2に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0050】まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ{Dc}Kcがこの形式で配信サーバ10より携帯電話またはパーソナルコンピュータのユーザに配布される。

【0051】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0052】さらに、配信サーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc-infが配布される。また、ライセンスとして、ライセンス鍵Kc、配信サーバ10からのライセンス鍵等を特定するための管理コードであるライセンスIDが配信サーバ10と携帯電話機100との間、または配信サーバ10とパーソナルコンピュータ50との間でやり取りされる。また、配信によらないライセンス、すなわち、ローカルでの使用を目的とするライセンスを特定するためにもライセンスIDは使用される。配信によるものと、ローカル使用のものとを区別するために、ライセンスIDの先頭は“0”で始まるものがローカル使用のライセンスIDであり、“0”以外から始まるものを配信によるライセンスIDであるとする。さらに、ライセンスとしては、コンテンツデータDcを識別するためのコードであるコンテンツIDや、コンテンツ供給者側の意向や利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード、またはライセンス管理デバイス）におけるライセンスのアクセスに対する制限に関する情報であるア

クセス制御情報ACmおよびデータ再生端末における再生に関する制御情報である再生制御情報ACp等が存在する。具体的には、アクセス制御情報ACmはメモリカード、およびライセンス管理デバイスからのライセンスまたはライセンス鍵を外部に出力するに当たっての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ACpは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0053】以後、コンテンツIDとライセンス鍵KcとライセンスIDとアクセス制御情報ACmと再生制御情報ACpとを併せて、ライセンスと総称することとする。

【0054】また、以降では、簡単化のためアクセス制御情報ACmは再生回数の制限を行なう制御情報である再生回数（0：再生不可、1～254：再生可能回数、255：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（1：移動複製可、2：移動のみ可、3：移動複製禁止）の2項目とし、再生制御情報ACpは再生可能な期限を規定する制御情報である再生期限（UTCtimeコード）のみを制限するものとする。

【0055】本発明の実施の形態においては、送信元の記録装置（メモリカード、またはライセンス管理デバイス）から受信先の記録装置へのライセンスの移動・複製において、送信元の記録装置に保持されたライセンスの有効・無効を示す有効フラグの運用を行なう。この有効フラグが有効であるとき、ライセンスをメモリカードから外部へ出すことが可能であることを意味し、有効フラグが無効であるとき、ライセンスをメモリカードから外部へ出すことができないことを意味する。

【0056】また、送信元の記録装置から受信先の記録装置へのライセンスの貸出／返却において、送信元の記録装置に保持されたライセンスが他の記録装置へ貸出が可能か否かを示す貸出フラグ、ライセンスの貸出先を特定するための情報である貸出先ID、および貸出したライセンスを識別するための識別情報である貸出時ライセンスIDの運用を行なう。

【0057】図4は、図1および図2に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0058】コンテンツ再生回路には固有の公開暗号鍵Kppyが設けられ、メモリカード、およびライセンス管理デバイスには固有の公開暗号鍵Kpmwが設けられる。そして、公開暗号鍵KppyおよびKpmwは、コンテンツ再生回路に固有の秘密復号鍵Kpyおよびメモリカード、ライセンス管理デバイスに固有の秘密復号鍵

Kmwによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0059】また、コンテンツ再生回路（携帯電話機、再生端末）のクラス証明書としてCpyが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてCmwが設けられる。これらのクラス証明書は、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスは、ライセンス取得の禁止対象となる。

【0060】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ{KPy/／Cpy}KPaの形式で、メモリカード、およびライセンス管理デバイスのクラス公開暗号鍵およびクラス証明書は認証データ{Kpmw/／Cmw}KPaの形式で出荷時にデータ再生回路、メモリカード、およびライセンス管理デバイスにそれぞれ記録される。後ほど詳細に説明するが、KPaは、配信システム全体で共通の公開認証鍵である。

【0061】また、メモリカード110、およびライセンス管理デバイスのデータ処理を管理するための鍵として、メモリカード、およびライセンス管理デバイスという媒体ごとに設定される公開暗号鍵Kpmcxと、公開暗号鍵Kpmcxで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Kmcxが存在する。このメモリカードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵Kpmcxを個別公開暗号鍵、秘密復号鍵Kmcxを個別秘密復号鍵と称する。

【0062】メモリカードとの、またはライセンス管理デバイスに対するデータ授受における秘密保持のための暗号鍵として、ライセンスの配信、および再生が行なわれるごとに配信サーバ10、携帯電話機100、メモリカード110、ライセンス管理デバイスにおいて生成される共通鍵Ks1～Ks3が用いられる。

【0063】ここで、共通鍵Ks1～Ks3は、配信サーバ、コンテンツ再生回路もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1～Ks3を「セッションキー」とも呼ぶこととする。

【0064】これらのセッションキーKs1～Ks3は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモリカード、およびライセンス管理デバイスによって全てのセッションにおいてセッションごとに発生し、セッションキーKs3は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0065】図5は、図1および図2に示した配信サーバ10の構成を示す概略ブロック図である。

【0066】配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツID等の配信情報を保持するための情報データベース304と、携帯電話やパーソナルコンピュータの各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、情報データベース304に保持されたコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0067】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカード、およびライセンス管理デバイスから送られてきた認証のための認証データ{Kpmw/／Cmw}KPaを復号するための2種類の公開認証鍵KPaを保持する認証鍵保持部313と、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ{Kpmw/／Cmw}KPaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵KPaまたはKpbによって復号処理を行なう復号処理部312と、配信セッションごとに、セッション鍵Ks1を発生するセッションキー発生部316、セッションキー発生部3



16より生成されたセッションキーKs1を復号処理部312によって得られたクラス公開暗号鍵Kpmwを用いて暗号化して、バスBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0068】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよびアクセス制御情報ACmを、復号処理部320によって得られたメモリカード、およびライセンス管理デバイスの個別公開暗号鍵Kpmcによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号化処理部328とを含む。

【0069】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0070】図6は、図1および図2に示したパーソナルコンピュータ50の構成を説明するための概略ブロック図である。パーソナルコンピュータ50は、パーソナルコンピュータ50の各部のデータ授受を行なうためのバスBS2と、パーソナルコンピュータ内を制御すると共に、各種のプログラムを実行するためのコントローラ(CPU)510と、データバスBS2と、データバスBS2に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク(HDD)530およびCD-ROMドライブ540と、ユーザからの指示を入力するためのキーボード560と、各種の情報を視覚的にユーザに与えるためのディスプレイ570とを含む。

【0071】パーソナルコンピュータ50は、さらに、暗号化コンテンツデータおよびライセンスを携帯電話機100等へ通信する際にコントローラ510と端子580との間でデータの授受を制御するためのUSBインタフェース550と、USBケーブル70を接続するための端子580と、配信サーバ10とインターネット網30を介して通信する際にコントローラ510と端子585との間でデータの授受を制御するためのモデム555と、インターネット網30と接続するための端子585とを含む。

【0072】コントローラ510は、プログラムであるライセンス管理モジュール511を実行することでインターネット網30を介して暗号化コンテンツデータおよびライセンスを配信サーバ10から取得するために、配信サーバ10との間でデータの授受を制御するとともに、CD-ROMドライブ540を介して音楽CDからリッピングによって暗号化コンテンツデータおよびライセンスを取得する際の制御を行なう。さらに、パーソナルコンピュータ50は、配信サーバ10からのライセン

スの受信を行なう際に配信サーバ10との間で、またはライセンス管理モジュール511からリッピングによるライセンスの受信を行なう際にはライセンス管理モジュール511との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス520とを含む。

【0073】図7は、図2に示した再生端末102の構成を説明するための概略ブロック図である。

【0074】再生端末102は、再生端末102の各部のデータ授受を行なうためのバスBS3と、バスBS3を介して再生端末102の動作を制御するためのコントローラ1106と、外部からの指示を再生端末102に与えるための操作パネル1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるための表示パネル1110とを含む。

【0075】再生端末102は、さらに、配信サーバ10からのコンテンツデータ(音楽データ)を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード110と、メモリカード110とバスBS3との間のデータの授受を制御するためのメモリカードインタフェース1200と、パーソナルコンピュータ50から暗号化コンテンツデータおよびライセンスを受信する際にバスBS3と端子1114との間のデータ授受を制御するためのUSBインタフェース1112と、USBケーブル70を接続するための端子1114とを含む。

【0076】再生端末102は、さらに、クラス公開暗号鍵Kpp1およびクラス証明書Cp1を公開認証鍵KPaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kpp1/Cp1}KPaを保持する認証データ保持部1500を含む。ここで、再生端末102のクラスyは、y=1であるとする。

【0077】再生端末102は、さらに、クラス固有の復号鍵であるKp1を保持するKp1保持部1502と、バスBS3から受けたデータをKp1によって復号し、メモリカード110によって発生されたセッションキーKs2を得る復号処理部1504とを含む。

【0078】再生端末102は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS3上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵Kcおよび再生制御情報ACpを受取る際に、セッションキー発生部1508により発生されたセッションキーKs3を復号処理部1504によって得られたセッションキーKs2によって暗号化し、バスBS3に出力する暗号化処理部1506とを含む。

【0079】再生端末102は、さらに、バスBS3上

のデータをセッションキーK s 3によって復号して、ライセンス鍵K cおよび再生制御情報A C pを出力する復号処理部1510と、バスB S 3より暗号化コンテンツデータ{D c} K cを受けて、復号処理部1510によって復号されたライセンス鍵K cによって暗号化コンテンツデータ{D c} K cを復号する復号処理部1516とを含む。

【0080】再生端末102は、さらに、復号処理部1516からの出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518の出力をデジタル信号からアナログ信号に変換するD A変換器1519と、D A変換器1519の出力をヘッドホンなどの外部出力装置(図示省略)へ出力するための端子1530とを含む。

【0081】なお、図7においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生回路1550を構成する。

【0082】一方、図1に示す携帯電話機100は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータあるいはライセンスの配信を受信する機能を有するものである。したがって、図1に示す携帯電話機100の構成は、図7に示す構成において、携帯電話網により無線伝送される信号を受信するためのアンテナと、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナに与えるための送受信部とマイクとスピーカと音声コーデック等の携帯電話機が本来備える機能を設けたものである。

【0083】携帯電話機100、再生端末102の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0084】図8は、図1および図2に示すメモリカード110の構成を説明するための概略ブロック図である。

【0085】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、K P m wおよびK m wが設けられ、メモリカードのクラス証明書C m wが設けられるが、メモリカード110においては、自然数w=3で表わされるものとする。また、メモリカードを識別する自然数xはx=4で表されるものとする。

【0086】したがって、メモリカード110は、認証データ{K P m 3//C m 3} K P aを保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵K m c 4を保持するK m c 保持部1402と、クラス秘密復号鍵K m 3を保持するK m 保持部1421と、個別秘密復号鍵K m c 4によって復号可能な公開暗号鍵K P m c 4を保持するK P m c 保持部1416とを含む。

【0087】このように、メモリカードという記録装置

の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0088】メモリカード110は、さらに、メモリカードインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスB S 4と、バスB S 4にインタフェース1424から与えられるデータから、クラス秘密復号鍵K m 3をK m 保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーK s 1を接点P aに出力する復号処理部1422と、K P a 保持部1414から公開認証鍵K P aを受けて、バスB S 4に与えられるデータから公開認証鍵K P aによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ1420に、得られたクラス公開鍵を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスB S 4に出力する暗号化処理部1406とを含む。

【0089】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーK s 2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーK s 2を復号処理部1408によって得られるクラス公開暗号鍵K P p yもしくはK P m wによって暗号化してバスB S 4に送出する暗号化処理部1410と、バスB S 4よりセッションキーK s 2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーK s 2によって復号する復号処理部1412と、暗号化コンテンツデータの再生セッションにおいてメモリ1415から読出されたライセンス鍵K cおよび再生制御情報A C pを、復号処理部1412で復号された他のメモリカード110の個別公開暗号鍵K P m c x (≠4)で暗号化する暗号処理部1417とを含む。

【0090】メモリカード110は、さらに、バスB S 4上のデータを個別公開暗号鍵K P m c 4と対をなすメモリカード110の個別秘密復号鍵K m c 4によって復号するための復号処理部1404と、暗号化コンテンツデータ{D c} K cと、暗号化コンテンツデータ{D c} K cを再生するためのライセンス(K c, A C p, A C m, ライセンスI D, コンテンツI D)と、有効フラグと、貸出先I Dと、貸出時ライセンスI Dと、付加情報D c - i n fと、メモリカード110内に格納される暗号化コンテンツデータを管理する再生リストファイルと、ライセンスを管理するためのライセンス管理ファイルとをバスB S 4より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモ

リによって構成される。また、メモリ 1415 は、ライセンス領域 1415 A と、データ領域 1415 B とから成る。ライセンス領域 1415 A は、ライセンス、有効フラグ、貸出先 ID、および貸出時ライセンス ID を記録するための領域である。データ領域 1415 B は、暗号化コンテンツデータ {Dc} Kc、暗号化コンテンツデータの関連情報 Dc-inf、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストファイルを記録するための領域である。そして、データ領域 1415 B は、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【0091】ライセンス領域 1415 A は、ライセンス（ライセンス鍵 Kc、再生制御情報 ACp、アクセス制限情報 ACm、ライセンス ID、コンテンツ ID）、有効フラグ、貸出先 ID、および貸出時ライセンス ID を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンス、有効フラグ、貸出先 ID、および貸出時ライセンス ID を格納する。ライセンス等に対してアクセスする場合には、ライセンス等が格納されている、あるいは、ライセンス等を記録したいエントリをエントリ番号によって指定する構成になっている。

【0092】メモリカード 110 は、さらに、バス BS4 を介して外部との間でデータ授受を行ない、バス BS4 との間で再生情報等を受けて、メモリカード 110 の動作を制御するためのコントローラ 1420 を含む。

【0093】なお、ライセンス領域 1415 A は、耐タンパモジュール領域に構成される。また、ライセンス領域 1415 A とデータ領域 1415 B とは、1つのメモリ 1415 内に構成されている必要はなく、それぞれ、別々に構成されていても良い。さらに、メモリ 1415 は、データ領域 1415 B を伴わないライセンス専用の領域であってもよい。

【0094】図 9 は、パーソナルコンピュータ 50 に内蔵されたライセンス管理デバイス 520 の構成を示す概略ブロック図である。ライセンス管理デバイス 520 は、メモリカード 110 におけるデータ領域 1415 B に相当する領域を必要としない点、インタフェース 1424 の機能および端子 1426 の形状が異なるインタフェース 5224 と端子 5226 とを備える点が異なるのみで、基本的にメモリカード 110 と同じ構成から成る。ライセンス管理デバイス 520 の認証データ保持部 5200、Kmc 保持部 5202、復号処理部 5204、暗号処理部 5206、復号処理部 5208、暗号処理部 5210、復号処理部 5212、KPa 保持部 5214、KPmc 保持部 5216、暗号処理部 5217、セッションキー発生部 5218、コントローラ 5220、Km

保持部 5221、復号処理部 5222、インタフェース 5224、端子 5226、切換スイッチ 5242、5246 は、それぞれ、メモリカード 110 の認証データ保持部 1400、Kmc 保持部 1402、復号処理部 1404、暗号処理部 1406、復号処理部 1408、暗号処理部 1410、復号処理部 1412、KPa 保持部 1414、KPmc 保持部 1416、暗号処理部 1417、セッションキー発生部 1418、コントローラ 1420、Km 保持部 1421、復号処理部 1422、切換スイッチ 1442、1446 と同じである。ただし、認証データ保持部 5200 は、認証データ {Kpm7/Cm7} KPa を保持し、KPmc 保持部 5216 は、個別公開暗号鍵 Kpm8 を保持し、Km 保持部 5202 は、クラス秘密復号鍵 Km7 を保持し、Kmc 保持部 5221 は、個別秘密復号鍵 Kmc8 を保持する。ライセンス管理デバイス 520 のクラスを表す自然数 w は w=7 であり、ライセンス管理デバイス 520 を識別するための自然数 x は x=8 であるとする。

【0095】ライセンス管理デバイス 520 は、ライセンス (Kc、ACp、ACm、ライセンス ID、コンテンツ ID) と、有効フラグと、貸出先 ID と、貸出時ライセンス ID とを記録するメモリ 5215 を、メモリカード 110 のメモリ 1415 に代えて含む。メモリ 5215 は、ライセンス、有効フラグ、貸出先 ID、および貸出時ライセンス ID を記録したライセンス領域 5215A を含む。

【0096】以下、図 1 および図 2 に示すデータ配信システムにおける各セッションの動作について説明する。

【0097】[配信] 図 10 および図 11 は、図 1 および図 2 に示すデータ配信システムのパーソナルコンピュータ 50 における暗号化コンテンツデータおよびライセンスの購入時に発生する配信セッションを説明するための第 1 および第 2 のフローチャートである。なお、この動作を「配信」と言う。

【0098】図 10 における処理以前に、パーソナルコンピュータ 50 のユーザは、配信サーバ 10 に対してインターネット網 30 を介して接続し、購入を希望するコンテンツに対するコンテンツ ID を取得していることを前提としている。

【0099】図 10 を参照して、パーソナルコンピュータ 50 のユーザからキーボード 560 を介してコンテンツ ID の指定による配信リクエストがなされる (ステップ S100)。そして、キーボード 560 を介して暗号化コンテンツデータのライセンスを購入するための購入条件 AC が入力される (ステップ S102)。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵 Kc を購入するために、暗号化コンテンツデータのアクセス制御情報 ACm、および再生制御情報 ACp を想定して購入条件 AC が入力される。

【0100】暗号化コンテンツデータの購入条件 AC が

入力されると、コントローラ 510 は、バス BS2 を介してライセンス管理デバイス 520 へ認証データの出力指示を与える（ステップ S104）。ライセンス管理デバイス 520 のコントローラ 5220 は、端子 5226、インタフェース 5224 およびバス BS5 を介して認証データの送信要求を受信する（ステップ S106）。そして、コントローラ 5220 は、バス BS5 を介して認証データ保持部 5200 から認証データ {K P m7 / / C m7} K P a を読み出し、{K P m7 / / C m7} K P a をバス BS5、インタフェース 5224 および端子 5226 を介して出力する（ステップ S108）。

【0101】パーソナルコンピュータ 50 のコントローラ 510 は、ライセンス管理デバイス 520 からの認証データ {K P m3 / / C m3} K P a に加えて、コンテンツ ID、ライセンス購入条件のデータ AC、および配信リクエストをモデム 555 およびインターネット網 30 を介して配信サーバ 10 に対して送信する（ステップ S110）。

【0102】配信サーバ 10 では、パーソナルコンピュータ 50 から配信リクエスト、コンテンツ ID、認証データ {K P m7 / / C m7} K P a、およびライセンス購入条件のデータ AC を受信し（ステップ S112）、復号処理部 312 においてライセンス管理デバイス 520 から出力された認証データを公開認証鍵 K P a で復号処理を実行する（ステップ S114）。

【0103】配信制御部 315 は、復号処理部 312 における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップ S116）。正当な認証データであると判断された場合、配信制御部 315 は、クラス公開暗号鍵 K P m7 およびクラス証明書 C m7 を承認し、受理する。そして、次の処理（ステップ S118）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵 K P m7 およびクラス証明書 C m7 を受理しないで配信セッションを終了する（ステップ S166）。

【0104】認証の結果、正当な認証データを持つライセンス管理デバイスを装着したパーソナルコンピュータからのアクセスであることが確認されると、配信サーバ 10 において、セッションキー発生部 316 は、配信のためのセッションキー K s1 を生成する（ステップ S118）。セッションキー K s1 は、復号処理部 312 によって得られたメモリカード 110 に対応するクラス公開暗号鍵 K P m7 によって、暗号化処理部 318 によって暗号化される（ステップ S120）。

【0105】配信制御部 315 は、ライセンス ID を生成し（ステップ S122）、ライセンス ID および暗号化されたセッションキー K s1 は、ライセンス ID / / {K s1} K m3 として、バス BS1 および通信装置 3

50 を介して外部に出力される（ステップ S124）。

【0106】パーソナルコンピュータ 50 が、ライセンス ID / / {K s1} K m7 を受信すると、コントローラ 510 は、ライセンス ID / / {K s1} K m7 をメモリカード 110 に入力する（ステップ S126）。そうすると、ライセンス管理デバイス 520 においては、端子 5226 およびインタフェース 5224 を介して、コントローラ 5220 は、ライセンス ID / / {K s1} K m7 を受理する（ステップ S128）。そして、コントローラ 5220 は、バス BS5 を介して {K s1} K m7 を復号処理部 5222 へ与え、復号処理部 5222 は、K m 保持部 5221 に保持されるライセンス管理デバイス 520 に固有なクラス秘密復号鍵 K m3 によって復号処理することにより、セッションキー K s1 を復号し、セッションキー K s1 を受理する（ステップ S130）。

【0107】コントローラ 5220 は、配信サーバ 10 で生成されたセッションキー K s1 の受理を確認すると、セッションキー発生部 5218 に対してライセンス管理デバイス 520 において配信動作時に生成されるセッションキー K s2 の生成を指示する。そして、セッションキー発生部 5218 は、セッションキー K s2 を生成する（ステップ S132）。

【0108】暗号化処理部 5206 は、切換スイッチ 5242 の接点 P a を介して復号処理部 5222 より与えられるセッションキー K s1 によって、切換スイッチ 5246 の接点を順次切換えることによって与えられるセッションキー K s2、および個別公開暗号鍵 K P m c 8 を 1 つのデータ列として暗号化して、{K s2 / / K P m c 8} K s1 をバス BS5 に出力する。バス BS5 に出力された暗号化データ {K s2 / / K P m c 8} K s1 は、バス BS5 からインタフェース 5224 および端子 5226 を介してパーソナルコンピュータ 50 に出力され（ステップ S134）、パーソナルコンピュータ 50 から配信サーバ 10 に送信される（ステップ S136）。

【0109】図 11 を参照して、配信サーバ 10 は、{K s2 / / K P m c 4} K s1 を受信して、復号処理部 320 においてセッションキー K s1 による復号処理を実行し、ライセンス管理デバイス 520 で生成されたセッションキー K s2、およびライセンス管理デバイス 520 に固有の公開暗号鍵 K P m c 8 を受理する（ステップ S138）。

【0110】配信制御部 315 は、ステップ S112 で取得したコンテンツ ID に従ってライセンス鍵 K c を情報データベース 304 から取得し（ステップ S140）、ステップ S112 で取得したライセンス購入条件のデータ AC に従って、アクセス制御情報 A C m および再生制御情報 A C p を決定する（ステップ S142）。

【0111】配信制御部 315 は、生成したライセン

ス、すなわち、ライセンスID、コンテンツID、ライセンス鍵Kc、再生制御情報ACp、およびアクセス制御情報ACmを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたライセンス管理デバイス520に固有の公開暗号鍵Kpmc8によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8を生成する(ステップS144)。そして、暗号化処理部328は、暗号化処理部326からの暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8を、復号処理部320からのセッションキーKs2によって暗号化し、暗号化データ{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を出力する。配信制御部315は、バスBS1および通信装置350を介して暗号化データ{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をパーソナルコンピュータ50へ送信する(ステップS146)。

【0112】パーソナルコンピュータ50は、送信された暗号化データ{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を受信し、バスBS2を介してライセンス管理デバイス520に入力する(ステップS148)。ライセンス管理デバイス520においては、端子5226およびインタフェース5224を介して、バスBS5に与えられた受信データを復号処理部5212によって復号する。復号処理部5212は、セッションキー発生部5218から与えられたセッションキーKs2を用いてバスBS5の受信データを復号し、バスBS5に出力する(ステップS150)。

【0113】この段階で、バスBS5には、Kmc保持部5202に保持される秘密復号鍵Kmc8で復号可能な暗号化ライセンス{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8が出力される(ステップS150)。

【0114】コントローラ5220の指示によって、暗号化ライセンス{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8は、復号処理部5204において、個別秘密復号鍵Kmc8によって復号され、ライセンス(ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)が受理される(ステップS152)。

【0115】パーソナルコンピュータ50のコントローラ510は、HDD530から読出したライセンス管理ファイルに基づいて、配信サーバ10から受信したライセンスを格納するためのエントリ番号を決定し、その決定したエントリ番号をバスBS2を介してライセンス管理デバイス520へ入力する。そして、コントローラ5

10は、ライセンス管理ファイルのライセンス管理情報を追加更新する(ステップS154)。

【0116】そうすると、ライセンス管理デバイス520のコントローラ5220は、ステップS152において取得したアクセス制御情報ACmに基づいて、取得したライセンスが貸出可能か否かを判定する(ステップS156)。アクセス制御情報ACmは、複製・移動制御情報と再生回数制御情報とから成る。複製・移動制御情報として「1」、「2」、および「3」のいずれかが設定されており、「1」はライセンスの複製・移動不可を意味し、「2」は複製不可・移動可を意味し、「3」は複製・移動禁止を意味する。また、再生回数制御情報としては、0~255の値が設定されている。そして、0~254の値は、設定された値の回数だけ暗号化コンテンツデータの再生が可能であることを意味し、255は、暗号化コンテンツデータを無制限に再生できることを意味する。本発明においては、複製・移動制御情報が「2」に設定され、かつ、再生回数制御情報が「255」に設定されているとき、ライセンスを貸出できるものとする。なお、再生回数制御情報が「255」に設定されていることは、ライセンスの貸出を可能にするための必須条件である。再生回数制御情報が「0~254」に設定されているときは、再生回数に制限があり、貸出元と貸出先とで何回、暗号化コンテンツデータを再生したかを管理するのは困難であるため再生回数が有限のときはライセンスの貸出を禁止し、再生回数が無限の場合に限りライセンスの貸出を可能にしたものである。

【0117】そして、コントローラ5220は、ライセンスの貸出が可能であれば、メモリ5215のライセンス領域5215Aのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する(ステップS158)。一方、ステップS156において、ライセンスの貸出が不可と判定されたとき、コントローラ5220は、ライセンス領域5215Aのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する(ステップS160)。

【0118】ステップS158またはステップS160の後、コントローラ5220は、ライセンス領域5215Aのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し(ステップS162)、ライセンス領域5215Aのエントリ番号によって指定された領域に、ステップS152において受理したライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、および再生制御情報ACp)を格納する(ステップS164)。そして、ライセンスの配信動作は終了する(ステップS166)。

【0119】ライセンスの配信動作が終了した後、パーソナルコンピュータ50のコントローラ510は、暗号化コンテンツデータの配信要求を配信サーバ10へ送信

し、配信サーバ10は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ10の配信制御部315は、情報データベース304より、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する。

【0120】パーソナルコンピュータ50は、{Dc}Kc//Dc-infを受信して、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受理する。そうすると、コントローラ1106は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを1つのコンテンツファイルとしてバスBS2を介してHDD530に入力する。また、コントローラ510は、ライセンス管理デバイス520に格納されたライセンスのエントリ番号と、平文のライセンスIDおよびコンテンツIDを含む暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、バスBS2を介してHDD530に入力する。さらに、コントローラ510は、HDD530に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Dc-infから抽出した暗号化コンテンツデータに関する情報(曲名、アーティスト名)等を追記し、全体の処理が終了する。

【0121】このようにして、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス520が正規の認証データを保持する機器であること、同時に、クラス証明書Cm7とともに暗号化して送信できた公開暗号鍵Kpm7が有効であることを確認した上でライセンスを配信することができ、不正なライセンス管理デバイスへのライセンスの配信を禁止することができる。

【0122】さらに、配信サーバおよびライセンスかんりデバイス520でそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0123】図1に示すデータ配信システムにおいて携帯電話機100に装着されたメモリカード110に対して、直接、ライセンスを配信する動作も図10および図11に示すフローチャートに従って行なわれる。すなわち、上記の説明において、パーソナルコンピュータ50を携帯電話機100に代え、ライセンス管理デバイス520をメモリカード110に代えれば良い。また、図10のステップS108においては、認証データ{Kpm7//Cm7}Kpaの代わりに認証データ{Kpm3//Cm3}Kpaがメモリカード110から出力される。その他は、上述したのと同じである。

【0124】[リッピング] パーソナルコンピュータ50のユーザは配信によって暗号化コンテンツデータとライセンスを取得する他に、所有する音楽CDから、音楽データを取得して利用することが可能である。著作権者の権利保護の立場から音楽CDのデジタル複製は自由に行なっても良いものではないが、個人が自己の使用目的のために、著作権保護機能を備えるツールを用いて複製し、音楽を楽しむことは許されている。そこで、ライセンス管理モジュール511は、音楽CDから音楽データを取得して、ライセンス管理モジュール511にて管理可能な暗号化コンテンツデータとライセンスとを生成するリッピング機能を実現するプログラムも含んでいる。

【0125】また、近年の音楽CDには、音楽データ内に、ウォーターマークと呼ばれる電子透かしを挿入したものがあある。このウォーターマークには、著作権者によって利用者における利用の範囲が利用規則として書込まれている。利用規則が書込まれている音楽データからのリッピングでは、著作権保護の点から必ずこの利用規則に従う必要がある。以後、利用規則として、複製条件(複製禁止・複製可能世代・複製可)、複製の有効期間、最大チェックアウト数、編集、再生速度、再生可能な地域コード、複製に対する再生回数制限、利用可能時間が記載されているとする。また、ウォーターマークが検出されない場合、すなわち、利用規則が書込まれていない従来の音楽CDもある。

【0126】また、リッピングは、音楽CDから、直接、音楽データを取得する他に、アナログ信号として入力された音楽信号を、デジタル化して音楽データとして取得する場合もある。さらには、データ量を減らすために圧縮符号化された音楽データを入力とすることも可能である。また、さらに、本実施の形態による配信システム以外の、配信システムにて配信されたコンテンツデータを入力として取り込むことも可能である。

【0127】図12および図13を参照して、音楽データが記録された音楽CDからのリッピングによる暗号化コンテンツデータおよびライセンスの取得について説明する。

【0128】図12は、図6に示すパーソナルコンピュータ50に含まれるCD-ROMドライブ540がCDから読出した音楽データをリッピングするソフトウェアの機能を示す機能ブロック図である。音楽データをリッピングするソフトウェアは、ウォーターマーク検出手段5400と、ウォーターマーク判定手段5401と、リマーク手段5402と、ライセンス発生手段5403と、音楽エンコーダ5404と、暗号手段5405とを備える。

【0129】ウォーターマーク検出手段5400は、音楽CDから取得した音楽データからウォーターマークを検出し、記載されている利用規則を抽出する。ウォーターマーク判定手段5401は、ウォーターマーク検出手段5400

0の検出結果、すなわち、ウォータマークが検出できたか否か、さらに検出できた場合には、ウォータマークで記載されていた利用規則に基づいて、リッピングの可否を判定する。この場合、リッピング可の場合、ウォータマークの利用規則が無い、または音楽CDに記録された音楽データの複製および移動が許可された利用規則がウォータマークによって記録されていたことを意味し、リッピング不可の場合、音楽CDに記録された音楽データを複製および移動してはいけない利用規則がウォータマークによって記録されていたことを意味する。

【0130】リマーク手段5402は、ウォータマーク判定手段5401における判定結果がリッピング可能で、複製世代の指示がある場合、つまり、音楽データを複製・移動して良い場合、音楽データに含まれるウォータマークを音楽データの複製条件を変更したウォータマークに付け替える。ただし、アナログ信号を入力してリッピングする場合や符号化された音楽データを入力とする場合、および他の配信システムにて配信された音楽データを入力とする場合には、リッピング可能であれば利用規則の内容に関わらず、必ず、ウォータマークを付け替える。この場合、複製世代の指示がある場合は、利用規則の内容を変更して、それ以外の場合には取得した利用規則をそのまま利用する。

【0131】ライセンス発生手段5403は、ウォータマーク判定手段5401の判定結果に基づいてライセンスを発生させる。音楽エンコーダ5404は、リマーク手段5402によってウォータマークがリマークされた音楽データを所定の方式に符号化する。暗号手段5405は、音楽エンコーダ5404からの音楽データをライセンス発生手段5403により発生されたライセンスに含まれるライセンス鍵Kcによって暗号化する。

【0132】図13を参照して、パーソナルコンピュータ50のコントローラ510におけるリッピング動作について説明する。リッピング動作が開始されると、ウォータマーク検出手段5400は、音楽CDから検出したデータに基づいてウォータマークの利用規則を検出する(ステップS800)。そして、ウォータマーク判定手段5401は、ウォータマーク検出手段5400の検出結果とウォータマークとして記録されていた利用規則に基づいて複製が可能か否かを判定する(ステップS802)。ウォータマークが検出され、利用規則によって複製が許可され、かつ、利用規則の内容がライセンス内のアクセス制御情報や再生制御情報にて対応可能な場合、リッピング可と判断され、ステップS804へ移行する。また、ウォータマークが検出され、利用規則によって複製の禁止、または、ライセンス内のアクセス制御情報や再生制御情報にて対応不可の利用規則が記載されている場合、リッピング禁止と判断され、ステップS828へ移行してリッピング動作は終了する。装着されたCDにウォータマークが含まれていない場合、ステップS

810へ移行する。

【0133】ステップS802において、リッピング可と判断した場合、音楽CDから音楽データが取込まれ、リマーク手段5402によって音楽データに含まれるウォータマークが複製条件を変更したウォータマークに付け替えられる(ステップS806)。すなわち、ウォータマークの利用規則が3世代までの複製を許可している場合、複製世代を2回にしたウォータマークに付け替える。そして、ライセンス発生手段5403は、利用規則を反映したライセンスを生成する。すなわち、ライセンス発生手段5403は、複製回数が2世代であるライセンスを生成する(ステップS806)。

【0134】一方、ステップS802において、ウォータマークが検出されない場合、ライセンス発生手段5403は、ライセンスの複製のみを禁止した移動・複製制御情報が「2」のライセンスを生成する(ステップS810)。

【0135】ステップS806またはS810の後、音楽エンコーダ5404は、ウォータマークがリマークされた音楽データを所定の方式に符号化してコンテンツデータDcを生成する(ステップS814)。そして、暗号手段5405は、音楽エンコーダ5404からの音楽データをライセンス発生手段5403により発生されたライセンスに含まれるライセンス鍵Kcによって暗号化を行ない、暗号化コンテンツデータ{Dc}Kcを生成する(ステップS816)。その後、音楽CDに含まれる情報またはパーソナルコンピュータ50のキーボード560から入力されたユーザ入力等によってコンテンツデータ{Dc}の付加情報Dc-infが生成される(ステップS818)。

【0136】そうすると、パーソナルコンピュータ50のコントローラ510は、バスBS2を介して暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得し、HDD530に記録する(ステップS820)。そして、コントローラ510は、生成されたライセンス(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生制御情報ACp)をライセンス管理デバイス520に格納する(ステップS822)。ライセンス管理デバイス520へのライセンスの格納は、コントローラ510上で実行されているライセンス管理モジュール511を介して図10および図11に示すフローチャートのステップS104からステップS166に従って行なわれる。すなわち、暗号化コンテンツデータおよびライセンスの配信における説明において配信サーバ10をコントローラ510に代えればよく、コントローラ510上で動作中のライセンス管理モジュール511は、配信サーバ10におけるライセンスの配信に対応する機能を実現できるプログラムである。その後、コントローラ510は、平文のトランザクションIDおよびコンテンツIDを含み、か

つ、HDDに記録した暗号化コンテンツデータ {Dc} Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、HDD530に記録する(ステップS824)。最後に、コントローラ510は、HDD530に記録されているコンテンツリストファイルに受理したコンテンツのファイル名を追記して(ステップS826)、リッピング動作が終了する(ステップS828)。

【0137】このように音楽CDからリッピングによっても暗号化コンテンツデータとライセンスとを取得でき、取得されたライセンスは、配信サーバ10から配信されたコンテンツとともに保護されて管理される。

【0138】このように、音楽CDからリッピングによって取得された暗号化コンテンツデータおよびライセンスは、ライセンス管理モジュール511によって生成され、配信サーバ10から受信した暗号化コンテンツデータおよびライセンスと同じように管理される。したがって、パーソナルコンピュータ50は、音楽CDからリッピングによって取得した暗号化コンテンツデータおよびライセンスを、後述するチェックアウトによって携帯電話機100または再生端末102に装着されたメモリカード110へ送信可能である。これによって、携帯電話機100または再生端末102のユーザは、パーソナルコンピュータ50がリッピングによって取得した暗号化コンテンツデータを自己のメモリカード110に受信して再生を楽しむことができる。

【0139】上記においては、パーソナルコンピュータ50は、音楽CDからリッピングによって暗号化コンテンツデータおよびライセンスを取得したが、本発明においては、これに限らず、他のインターネット配信によって受信したコンテンツデータからリッピングによって暗号化コンテンツデータおよびライセンスを生成しても良い。

【0140】[移動] 上述したように、メモリカード110およびライセンス管理デバイス520は、配信サーバ10から暗号化コンテンツデータおよびライセンスを取得できる。そこで、メモリカード110またはライセンス管理デバイス520が配信サーバ10から受信したライセンスを他のメモリカードへ移動するときの動作について説明する。

【0141】図14および図15は、図1および図2に示すデータ配信システムにおいて、ライセンス管理デバイス520が配信サーバ10から受信した暗号化コンテンツデータおよびライセンスを携帯電話機100または再生端末102に装着されたメモリカード110へ移動する動作を説明するための第1および第2のフローチャートである。携帯電話機100または再生端末102は、移動においては、データの中継を行なうのみの機器であるため、フローチャートから省略してある。移動を説明するに当たり、図1の携帯電話機100に装着され

たメモリカード110へ移動する場合について説明を行なうが、図2の再生端末102に装着されたメモリカード110へ移動する場合についても同様であり、携帯電話機100を再生端末102に読替えば良い。また、メモリカード110からライセンス管理デバイス520へ移動する場合も同様に、ライセンス管理デバイス520とメモリカード110とを読替えばよい。

【0142】なお、図14における処理以前に、パーソナルコンピュータ50のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。また、コントローラ510は、ライセンス管理ファイルを保持していることを前提としている。

【0143】図14を参照して、パーソナルコンピュータ50のキーボード560から移動リクエストが入力されると(ステップS300)、コントローラ510は、USBインタフェース550、端子580、およびUSBケーブル70を介して認証データの送信要求をメモリカード110へ送信する(ステップS302)。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する(ステップS304)。

【0144】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ {K P m 3 / / C m 3} K P a をバスBS4を介して読出し、その読出した認証データ {K P m 3 / / C m 3} K P a をバスBS4、インタフェース1424および端子1426を介して外部へ出力する(ステップS306)。そして、パーソナルコンピュータ50のコントローラ510は、端子580およびUSBインタフェース550を介して認証データ {K P m 3 / / C m 3} K P a を受取り、バスBS2を介してライセンス管理デバイス520へ認証データ {K P m 3 / / C m 3} K P a を送信する(ステップS308)。

【0145】そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226およびインタフェース5224を介して認証データ {K P m 3 / / C m 3} K P a を受信し、その受信した認証データ {K P m 3 / / C m 3} K P a をバスBS5を介して復号処理部5208へ与える。そして、復号処理部5208は、K P a 保持部5214からの認証鍵K P a によって認証データ {K P m 3 / / C m 3} K P a の復号処理を実行する(ステップS310)。コントローラ5220は、復号処理部5208における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからのクラス公開暗号鍵K P m 3 とクラス証明書C m 3 とを保持することを認証するために、正規の機関でその正当性を証明するための暗



号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップS312）。正当な認証データであると判断された場合、コントローラ5220は、クラス公開暗号鍵K<sub>Pm3</sub>およびクラス証明書C<sub>m3</sub>を承認し、受理する。そして、次の処理（ステップS314）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K<sub>Pm3</sub>およびクラス証明書C<sub>m3</sub>を受理しないで処理を終了する（ステップS374）。

【0146】認証の結果、正当な認証データを持つメモリカードであることが確認されると、ライセンス管理デバイス520において、コントローラ5220は、セッションキー発生部5218を制御し、セッションキー発生部5218は、移動のためのセッションキーK<sub>s2a</sub>を生成する（ステップS314）。セッションキーK<sub>s2a</sub>は、復号処理部5208によって得られたメモリカード110に対応するクラス公開暗号鍵K<sub>Pm3</sub>によって、暗号化処理部5210によって暗号化される。そして、コントローラ5220は、バスBS5を介して暗号化データ{K<sub>s2a</sub>}Km3を取得し、バスBS5、インタフェース5224および端子5226を介して暗号化データ{K<sub>s2a</sub>}Km3を出力する（ステップS316）。

【0147】コントローラ510は、バスBS2を介して{K<sub>s2a</sub>}Km3をライセンス管理デバイス520から受理し（ステップS318）、HDD530に記録されているライセンス管理情報からライセンスIDを取得する（ステップS320）。そして、コントローラ510は、取得したライセンスIDと、ステップS318において受理した暗号化データ{K<sub>s2a</sub>}Km3とを1つのデータにしてライセンスID//{K<sub>s2a</sub>}Km3を端子580およびUSBインタフェース550を介して携帯電話機100に装着されたメモリカード110へ送信する（ステップS322）。そうすると、メモリカード110のコントローラ1106は、端子1426、インタフェース1424、およびバスBS4を介してライセンスID//{K<sub>s2a</sub>}Km3を受理する

（ステップS324）。その後、コントローラ1420は、暗号化データ{K<sub>s2a</sub>}Km3を復号処理部1422へ与え、復号処理部1422は、Km保持部1421からのクラス秘密復号鍵Km3によって{K<sub>s2a</sub>}Km3を復号してセッションキーK<sub>s2a</sub>を受理する（ステップS326）。そして、セッションキー発生部1418は、セッションキーK<sub>s2b</sub>を生成し（ステップS328）、暗号化処理部1406は、切換スイッチ1446の端子を順次切換えることによって取得したセッションキーK<sub>s2b</sub>、および個別公開暗号鍵K<sub>Pmc4</sub>を、復号処理部1404によって復号されたセッションキーK<sub>s2a</sub>によって暗号化し、暗号化データ{K<sub>s2b</sub>//K<sub>Pmc4</sub>}K<sub>s2a</sub>を生成する。コントロー

ラ1420は、暗号化データ{K<sub>s2b</sub>//K<sub>Pmc4</sub>}K<sub>s2a</sub>をバスBS4、インタフェース1424および端子1426を介して出力し（ステップS330）、パーソナルコンピュータ50のコントローラ510は、端子580およびUSBインタフェース550を介して暗号化データ{K<sub>s2b</sub>//K<sub>Pmc4</sub>}K<sub>s2a</sub>を受理する。そして、コントローラ510は、暗号化データ{K<sub>s2b</sub>//K<sub>Pmc4</sub>}K<sub>s2a</sub>をバスBS2を介してライセンス管理デバイス520へ送信する（ステップS332）。

【0148】そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS5を介して暗号化データ{K<sub>s2b</sub>//K<sub>Pmc4</sub>}K<sub>s2a</sub>を受信し、その受信した暗号化データ{K<sub>s2b</sub>//K<sub>Pmc4</sub>}K<sub>s2a</sub>を復号処理部5212に与える。復号処理部5212は、セッションキー発生部5218からのセッションキーK<sub>s2a</sub>によって暗号化データ{K<sub>s2b</sub>//K<sub>Pmc4</sub>}K<sub>s2a</sub>を復号し、セッションキーK<sub>s2b</sub>、および公開暗号鍵K<sub>Pmc4</sub>を受理する（ステップS334）。

【0149】その後、コントローラ510は、ライセンス管理デバイス520に対応するライセンス管理情報から移動の対象となっているライセンスが格納されているエントリ番号を取得し（ステップS336）、その取得したエントリ番号とライセンスの移動要求とをライセンス管理デバイス520へ入力する（ステップS338）。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介してエントリ番号とライセンスの移動要求とを受信し、その受信したエントリ番号によって指定されるメモリ5215のライセンス領域5215Aのエントリからライセンス（ライセンスID、コンテンツID、ライセンス鍵K<sub>c</sub>、アクセス制御情報A<sub>Cm</sub>、再生制御情報A<sub>Cp</sub>）を取得する（ステップS340）。

【0150】図15を参照して、コントローラ5220は、ステップS340において取得したライセンスの貸出の有無を貸出フラグによって判定する（ステップS342）。そして、取得したライセンスが貸出中であれば、移動動作は終了する（ステップS374）。取得したライセンスが貸出中でなければ、コントローラ5220は、次いで、アクセス制御情報A<sub>Cm</sub>を確認する（ステップS344）。つまり、コントローラ5220は、取得したアクセス制御情報A<sub>Cm</sub>に基づいて、最初に、メモリカード110へ移動しようとするライセンスが再生回数によって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数が残っていない場合（再生回数=0）、暗号化コンテンツデータをライセンスによって再生することができ

ず、その暗号化コンテンツデータとライセンスとをメモリカード110へ移動する意味がないからである。再生することができない場合、再生することができる場合、移動・複製制御情報によって、ライセンスの複製、移動の可否を判断する。

【0151】ステップS344において、暗号化コンテンツデータの再生回数ができない（再生回数＝0）、または、移動・複製フラグが移動複製禁止（＝0）の場合、アクセス制御情報ACmによって、複製移動不可と判断し、ステップS374へ移行し、移動動作は終了する。ステップS344において、暗号化コンテンツデータの再生ができ（再生回数≠0）、かつ、移動・複製制御情報が移動のみ可「＝2」の場合、ライセンスの移動であると判断され、コントローラ5220は、メモリ5215のライセンス領域5215Aにおいて指定されたエントリ番号内の有効フラグを無効する（ステップS346）。また、暗号化コンテンツデータの再生ができ「再生回数≠0」、かつ、移動・複製制御情報が複製可の場合、ライセンスの複製であると判断され、ステップS346を行わずにステップS348へ移行する。

【0152】ステップS344またはステップS346の後、暗号化処理部5217は、復号処理部5212によって得られたメモリカード110に固有の公開暗号鍵KPmc4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成する（ステップS348）。このように、ライセンスの移動が可能となるときは、ライセンス領域5215Aの有効フラグを無効にしてから（ステップS346参照）、ステップS348の処理を行なうが、ライセンスの複製が許可されている場合は、複製元と複製先との両方においてライセンスを使用可能にするためにライセンスの有効フラグを無効にするステップS346を介さずにステップS348へ移行するようにしたものである。したがって、ライセンスを移動させたときは、ライセンス管理デバイス520からライセンスを読出すことはできない。

【0153】そして、暗号化処理部5206は、暗号化処理部5217によって暗号化された暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をスイッチ5246の接点Pcを介して受取り、復号処理部5212によって復号されたセッションキーKs2bをスイッチ5242の接点Pbを介して受取り、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をセッションキーKs2bによって暗号化する。そして、コントローラ5220は、暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをバスBS5、インタフェース5224、および端子5226を介して出力する（ステップS350）。

【0154】コントローラ510は、バスBS2を介してメモリカード120から暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを受取り、その受取った暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをメモリカード110へ送信する（ステップS352）。

【0155】メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bの入力を受けて、暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを復号処理部1412へ与える。そして、復号処理部1412は、暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをバスBS4を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2bによって復号し、{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を受取り（ステップS354）。

【0156】その後、コントローラ1420の指示によって、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4は、復号処理部1404において、秘密復号鍵Kmc4によって復号され、ライセンス（ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp）が受取られる（ステップS356）。

【0157】そうすると、コントローラ510は、受信側であるメモリカード110のライセンス管理情報から移動/複製されたライセンスを格納するためのエントリ番号を決定し、メモリカード110に入力するとともに、受信側（メモリカード110）のライセンス管理情報を更新する（ステップS358）。

【0158】そうすると、メモリカード100のコントローラ1420は、ステップS356において取得したアクセス制御情報ACmに基づいて、取得したライセンスが貸出可能か否かを判定する（ステップS360）。そして、コントローラ1420は、ライセンスの貸出が可能であれば、メモリ1415のライセンス領域1415Aのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する（ステップS362）。一方、ステップS360において、ライセンスの貸出が不可と判定されたとき、コントローラ1420は、ライセンス領域1415Aのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する（ステップS364）。

【0159】ステップS362またはステップS364の後、コントローラ1420は、ライセンス領域141

5Aのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し（ステップS366）、ライセンス領域1415Aのエントリ番号によって指定された領域に、ステップS356において受理したライセンス（ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、および再生制御情報ACp）を格納する（ステップS368）。

【0160】一方、ステップS358の後、コントローラ510は、ライセンスの移動または複製が可能かを判定し（ステップS370）、移動可能であるとき、送信側のライセンス管理情報、すなわち、移動したライセンスに対応するHDD530に記録されているライセンス管理情報を削除し、送信側のライセンス管理情報およびメモリカード110のデータ領域1415Bに記録されているライセンス管理ファイルを書換える（ステップS372）。ステップS370において、ライセンスの貸出が可能と判定されたとき、またはステップS372の後、またはステップS368の後、ライセンスの移動動作は終了する（ステップS374）。

【0161】なお、暗号化コンテンツデータのメモリカード120からメモリカード110への移動は、ライセンスの移動が終了した後、メモリカード120のデータ領域1415Bから暗号化コンテンツデータを読み出してメモリカード110へ送信することによって行なえば良い。

【0162】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵Kpm3が有効であることを確認した上で、正規なメモリカードへの移動要求に対してのみライセンスを移動することができ、不正なメモリカードへの移動を禁止することができる。

【0163】また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの移動の動作におけるセキュリティを向上させることができる。

【0164】また、メモリカード110からライセンス管理デバイス520へのライセンスの移動も、図14および図15に示すフローチャートに従って行なわれる。つまり、図1において、携帯電話機100によって配信を受け、メモリカード110に格納した暗号化コンテンツデータとライセンスとをパーソナルコンピュータ50へ退避できることになる。

【0165】また、パーソナルコンピュータ50が配信サーバ10から受信したライセンスをメモリカード110へ移動できるのは、ライセンス管理デバイス520が配信サーバ10からハード的に受信したライセンスだけ

であり、音楽CDからライセンス管理モジュール511によってリッピングされたライセンスは移動できない。そこで、次に説明するチェックアウト（貸出）およびチェックイン（返却）の概念によって、ライセンス管理モジュール511によってリッピングし、ライセンス管理デバイス520に記録したライセンスをメモリカード110へ送信できるようにした。

【0166】また、メモリカード120からメモリカード110へのライセンスの貸出、および返却も可能である。「移動」と「貸出」との相違は、「移動」は、ライセンスを移動させた送信元のメモリカードにおいては、ライセンスの有効フラグが無効に設定されている（図15のステップS346参照）ため、「移動」は、送信元のメモリカードから暗号化コンテンツデータおよびライセンスを取得して暗号化コンテンツデータの再生を行なうことができないが、「貸出」は、ライセンスを貸出した貸出元のメモリカードから暗号化コンテンツデータおよびライセンスを取得して暗号化コンテンツデータの再生を行なうことができる点にある。また、上述したように、音楽CDからリッピングしたライセンスを送る。

【0167】「貸出」図1および図2に示すデータ配信システムにおいて、配信サーバ10からライセンス管理デバイス520へ配信された、あるいは音楽CDからリッピングされた暗号化コンテンツデータおよびライセンスをメモリカード110に返却を前提として貸出するために送信する動作について説明する。なお、この動作を「貸出」という。

【0168】図16および図17は、ライセンス管理デバイス520からメモリカード110へのライセンスの貸出を説明するための第1および第2のフローチャートである。

【0169】なお、図16における処理以前に、携帯電話機100のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。また、コントローラ40は、ライセンス管理ファイルを保持していることを前提としている。

【0170】図16を参照して、パーソナルコンピュータ50のキーボード560から貸出リクエストが入力されると（ステップS400）、コントローラ510は、携帯電話機100を介して認証データの送信要求をメモリカード110へ送信する（ステップS402）。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する（ステップS404）。

【0171】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{Kpm3／／Cm3}KpaをバスBS4を

介して読出し、その読出した認証データ {K P m 3 / / C m 3} K P a をバス B S 4、インタフェース 1 4 2 4 および端子 1 4 2 6 を介して外部へ出力する（ステップ S 4 0 6）。そして、パーソナルコンピュータ 5 0 のコントローラ 5 1 0 は、端子 5 8 0 および USB インタフェース 5 5 0 を介して認証データ {K P m 3 / / C m 3} K P a を受取り、バス B S 2 を介してライセンス管理デバイス 5 2 0 へ認証データ {K P m 3 / / C m 3} K P a を送信する（ステップ S 4 0 8）。

【0172】そうすると、ライセンス管理デバイス 5 2 0 のコントローラ 5 2 2 0 は、端子 5 2 2 6 およびインタフェース 5 2 2 4 を介して認証データ {K P m 3 / / C m 3} K P a を受信し、その受信した認証データ {K P m 3 / / C m 3} K P a をバス B S 5 を介して復号処理部 5 2 0 8 へ与える。そして、復号処理部 5 2 0 8 は、K P a 保持部 5 2 1 4 からの認証鍵 K P a によって認証データ {K P m 3 / / C m 3} K P a の復号処理を実行する（ステップ S 4 1 0）。コントローラ 1 4 2 0 は、復号処理部 5 2 0 8 における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード 1 1 0 が正規のメモリカードからのクラス公開暗号鍵 K P m 3 とクラス証明書 C m 3 とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップ S 4 1 2）。正当な認証データであると判断された場合、コントローラ 5 2 2 0 は、クラス公開暗号鍵 K P m 3 およびクラス証明書 C m 3 を承認し、受理する。そして、次の処理（ステップ S 4 1 4）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵 K P m 3 およびクラス証明書 C m 3 を受理しないで処理を終了する（ステップ S 4 7 8）。

【0173】認証の結果、正当な認証データを持つメモリカードからのアクセスであることが確認されると、ライセンス管理デバイス 5 2 0 において、コントローラ 5 2 2 0 は、セッションキー発生部 5 2 1 8 を制御し、セッションキー発生部 5 2 1 8 は、貸出のためのセッションキー K s 2 a を生成する（ステップ S 4 1 4）。セッションキー K s 2 a は、復号処理部 5 2 0 8 によって得られたメモリカード 1 1 0 に対応するクラス公開暗号鍵 K P m 3 によって、暗号化処理部 5 2 1 0 によって暗号化される。そして、コントローラ 5 2 2 0 は、バス B S 5 を介して暗号化データ {K s 2 a} K m 3 を取得し、バス B S 5、インタフェース 5 2 2 4 および端子 5 2 2 6 を介して暗号化データ {K s 2 a} K m 3 を出力する（ステップ S 4 1 6）。

【0174】コントローラ 5 1 0 は、バス B S 2 を介して {K s 2 a} K m 3 を送信側から受理し（ステップ S 4 1 8）、送信側のライセンス管理情報、すなわち、H D D 5 3 0 に記録されている貸出を行なうライセンスに

対応するライセンス ID を取得する（ステップ S 4 2 0）。そして、コントローラ 5 1 0 は、取得したライセンス ID と、ステップ S 4 1 8 において受理した暗号化データ {K s 2 a} K m 3 とを 1 つにデータにしてライセンス ID / / {K s 2 a} K m 3 を端子 5 8 0 および USB インタフェース 5 5 0 を介してメモリカード 1 1 0 へ送信する（ステップ S 4 2 2）。そうすると、メモリカード 1 1 0 のコントローラ 1 4 2 0 は、端子 1 4 2 6、インタフェース 1 4 2 4、およびバス B S 4 を介してライセンス ID / / {K s 2 a} K m 3 を受理する（ステップ S 4 2 4）。その後、コントローラ 1 4 2 0 は、暗号化データ {K s 2 a} K m 3 を復号処理部 1 4 2 2 へ与え、復号処理部 1 4 2 2 は、K m 保持部 1 4 2 1 からのクラス秘密復号鍵 K m 3 によって {K s 2 a} K m 3 を復号してセッションキー K s 2 a を受理する（ステップ S 4 2 6）。そして、セッションキー発生部 1 4 1 8 は、セッションキー K s 2 b を生成し（ステップ S 4 2 8）、暗号化処理部 1 4 0 6 は、切換スイッチ 1 4 4 6 の端子を順次切換えることによって取得したセッションキー K s 2 b、および個別公開暗号鍵 K P m c 4 を、復号処理部 1 4 0 4 によって復号されたセッションキー K s 2 a によって暗号化し、暗号化データ {K s 2 b / / K P m c 4} K s 2 a を生成する。コントローラ 1 4 2 0 は、暗号化データ {K s 2 b / / K P m c 4} K s 2 a をバス B S 4、インタフェース 1 4 2 4 および端子 1 4 2 6 を介して出力し（ステップ S 4 3 0）、コントローラ 5 1 0 は、端子 5 8 0 および USB インタフェース 5 5 0 を介して暗号化データ {K s 2 b / / K P m c 4} K s 2 a を受理する。そして、コントローラ 5 1 0 は、暗号化データ {K s 2 b / / K P m c 4} K s 2 a をバス B S 2 を介してライセンス管理デバイス 5 2 0 へ入力する（ステップ S 4 3 2）。

【0175】そうすると、ライセンス管理デバイス 5 2 0 のコントローラ 5 2 2 0 は、端子 5 2 2 6、インタフェース 5 2 2 4 およびバス B S 5 を介して暗号化データ {K s 2 b / / K P m c 4} K s 2 a を受信し、その受信した暗号化データ {K s 2 b / / K P m c 4} K s 2 a を復号処理部 5 2 1 2 に与える。復号処理部 5 2 1 2 は、セッションキー発生部 5 2 1 8 からのセッションキー K s 2 a によって暗号化データ {K s 2 b / / K P m c 4} K s 2 a を復号し、セッションキー K s 2 b、および公開暗号鍵 K P m c 4 を受理する（ステップ S 4 3 4）。

【0176】その後、コントローラ 5 1 0 は、貸出を行なうライセンスに対応したライセンス管理情報から移動の対象となっているライセンスが格納されているエントリ番号を取得し（ステップ S 4 3 6）、貸出用ライセンス ID を生成し（ステップ S 4 3 8）、ステップ S 4 3 6 において取得したエントリ番号とステップ S 4 3 8 において生成した貸出用ライセンス ID とによって指定さ

れたライセンスの貸出要求をライセンス管理デバイス520へ入力する(ステップS440)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介してエントリ番号、貸出用ライセンスID、およびライセンスの貸出要求とを受信し、その受信したエントリ番号によって指定されるメモリ1415のライセンス領域5215Aのエントリからライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、再生制御情報ACp)を取得する(ステップS442)。

【0177】コントローラ5220は、取得したアクセス制御ACmによってライセンスの複製が可能か否かを判定し(ステップS444)、複製可であれば図17のステップS452へ移行し、複製が禁止されていれば図17のステップS446へ移行する。

【0178】図17を参照して、ステップS444においてライセンスの複製が禁止されていると判定されたとき、ステップS442において取得したライセンスの貸出可否を貸出フラグによって判定する(ステップS446)。そして、取得したライセンスが貸出不可であれば、貸出動作は終了する(ステップS478)。取得したライセンスが貸出可でなければ、コントローラ5220は、指定されたエントリ内の貸出フラグを「貸出中」に変更し、受理した貸出用ライセンスIDを貸出時ライセンスIDの欄に格納し、ステップS434において受理した公開暗号鍵Kpmc4を貸出先IDの欄に格納する(ステップS448)。そして、コントローラ5220は、移動・複製禁止を設定した(移動・複製制御情報が「3」である)貸出用アクセス制御情報ACmを生成し、受理した貸出用ライセンスIDと生成した貸出用アクセス制御情報ACmとを、指定されたエントリから取得したライセンスIDおよびアクセス制御情報ACmと置換する(ステップS450)。これによって、メモリカード110へ貸出されるライセンス(貸出用ライセンスID、コンテンツID、ライセンス鍵Kc、貸出用アクセス制御情報ACm、再生制御情報ACp)が生成されるとともに、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Aには、元のライセンス(貸出用ライセンスID、コンテンツID、ライセンス鍵Kc、貸出用アクセス制御情報ACm、再生制御情報ACp)が格納されたままである。そして、ライセンス管理デバイス520のライセンス領域5215Aに格納されたままのライセンスは、メモリカード110へ貸出される。このため、ライセンス管理デバイス520には、移動の場合と異なりライセンスが残るためライセンスのバックアップとして機能する。

【0179】ステップS444において複製可と判定されたとき、またはステップS450の後、暗号化処理部5217は、復号処理部5212によって得られたメモ

リカード110に固有の公開暗号鍵Kpmc4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成する(ステップS452)。なお、ステップS444においてライセンスの複製が可能と判定されたとき、ステップS442において取得されたライセンスが公開暗号鍵Kpmc4によって暗号化される。

【0180】そして、暗号化処理部5206は、暗号化処理部5217によって暗号化された暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をスイッチ5246の接点Pcを介して受取り、復号処理部5212によって復号されたセッションキーKs2bをスイッチ5242の接点Pbを介して受取り、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をセッションキーKs2bによって暗号化する。そして、コントローラ5220は、暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをバスBS5、インタフェース5224、および端子5226を介して出力する(ステップS454)。

【0181】コントローラ510は、バスBS2を介してメモリカード120から暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを受取り、その受理した暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを携帯電話機100に装着された貸出先のメモリカード110へ入力する(ステップS456)。

【0182】メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bの入力を受けて、暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを復号処理部1412へ与える。そして、復号処理部1412は、暗号化データ{ {ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをバスBS4を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2bによって復号し、{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を受理する(ステップS458)。

【0183】その後、コントローラ1420の指示によって、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4は、復号処理部1404において、秘密復号鍵Kmc4によって復号され、ライセンス(ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)が受理される(ステップS46

0)。

【0184】そうすると、コントローラ510は、受信側であるメモリカード110のライセンス管理情報から移動／複製されたライセンスを格納するためのエントリ番号を決定し、メモリカード110に入力するとともに、受信側のライセンス管理情報を更新する(ステップS462)。

【0185】そうすると、メモリカード100のコントローラ1420は、ステップS460において取得したアクセス制御情報ACmに基づいて、取得したライセンスが貸出可能か否かを判定する(ステップS464)。そして、コントローラ1420は、ライセンスの貸出が可能であれば、メモリ1415のライセンス領域1415Aのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する(ステップS466)。一方、ステップS360において、ライセンスの貸出が不可と判定されたとき、コントローラ1420は、ライセンス領域1415Aのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する(ステップS468)。貸出においては、ステップS450においてアクセス制御情報の移動・複製制御情報が移動・複製不可に設定されてライセンス管理デバイス520から出力されるため必ずステップS468へ進む。

【0186】ステップS466またはステップS468の後、コントローラ1420は、ライセンス領域1415Aのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し(ステップS470)、ライセンス領域1415Aのエントリ番号によって指定された領域に、ステップS460において受理したライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、および再生制御情報ACp)を格納する(ステップS472)。

【0187】一方、ステップS462の後、コントローラ510は、ライセンスの移動または複製が可能か否かを判定し(ステップS474)、移動可能であるとき、貸出先のライセンス管理情報に貸出用ライセンスIDを追記し、貸出先ライセンス管理情報を更新する(ステップS476)。ステップS474において、ライセンスの貸出が可能と判定されたとき、またはステップS476の後、またはステップS472の後、ライセンスの貸出動作は終了する(ステップS478)。

【0188】なお、暗号化コンテンツデータのメモリカード110への貸出は、ライセンスの移動が終了した後、コントローラ510がHDD530から暗号化コンテンツデータを読み出してメモリカード110へ送信することによって行なえば良い。

【0189】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信でき

た公開暗号鍵Kpm3が有効であることを確認した上で、正規なメモリカードへの貸出要求に対してのみライセンスを貸出を行なうことができ、不正なメモリカードへの貸出を禁止することができる。

【0190】また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの貸出動作におけるセキュリティを向上させることができる。

【0191】[返却] 図16および図17を参照して説明したライセンス管理デバイス520からメモリカード110へ貸出されたライセンスをメモリカード110からライセンス管理デバイス520へ返却する動作について説明する。

【0192】図18～図21は、メモリカード110からライセンス管理デバイス520へライセンスを返却する動作を説明するための第1～第4のフローチャートである。

【0193】なお、図18における処理以前に、ユーザは、パーソナルコンピュータ50にUSBケーブル70によって接続された携帯電話機100に装着されたメモリカード110から返却されるライセンスおよびコンテンツをHDD530に記録されているコンテンツリストファイルに従って決定し、返却側のコンテンツファイルと貸出側および返却側の双方のライセンス管理ファイルとが特定できていることを前提として説明する。

【0194】図18を参照して、パーソナルコンピュータ50のキーボード560から返却リクエストが入力されると(ステップS500)、コントローラ510は、端子580およびUSBインタフェース550を介して認証データの送信要求をメモリカード110へ送信する(ステップS502)。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する(ステップS504)。

【0195】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{Kpm3／／Cm3}KpaをバスBS4を介して読み出し、その読み出した認証データ{Kpm3／／Cm3}KpaをバスBS4、インタフェース1424および端子1426を介してコントローラ510へ出力する(ステップS506)。そして、コントローラ510は、端子580およびUSBインタフェース550を介して認証データ{Kpm3／／Cm3}Kpaを受取り、バスBS2を介してライセンス管理デバイス520へ認証データ{Kpm3／／Cm3}Kpaを送信する(ステップS508)。

【0196】そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226およびイン

タフェース 5224 を介して認証データ {K P m 3 / / C m 3} K P a を受信し、その受信した認証データ {K P m 3 / / C m 3} K P a をバス B S 5 を介して復号処理部 5208 へ与える。そして、復号処理部 5208 は、K P a 保持部 5214 からの認証鍵 K P a によって認証データ {K P m 3 / / C m 3} K P a の復号処理を実行する (ステップ S 510)。コントローラ 5220 は、復号処理部 5208 における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード 110 が正規のメモリカードからのクラス公開暗号鍵 K P m 3 とクラス証明書 C m 3 とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう (ステップ S 512)。正当な認証データであると判断された場合、コントローラ 5220 は、クラス公開暗号鍵 K P m 3 およびクラス証明書 C m 3 を承認し、受理する。そして、次の処理 (ステップ S 514) へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵 K P m 3 およびクラス証明書 C m 3 を受理しないで処理を終了する (ステップ S 638)。

【0197】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであることが確認されると、ライセンス管理デバイス 520 において、コントローラ 5220 は、セッションキー発生部 5218 を制御し、セッションキー発生部 5218 は、返却のためのセッションキー K s 2 a を生成する (ステップ S 514)。セッションキー K s 2 a は、復号処理部 5208 によって得られたメモリカード 110 に対応するクラス公開暗号鍵 K P m 3 によって、暗号化処理部 1410 によって暗号化される。そして、コントローラ 5220 は、バス B S 5 を介して暗号化データ {K s 2 a} K m 3 を取得し、バス B S 5、インタフェース 5224 および端子 5226 を介して暗号化データ {K s 2 a} K m 3 を出力する (ステップ S 516)。

【0198】コントローラ 510 は、バス B S 2 を介して {K s 2 a} K m 3 をライセンス管理デバイス 520 から受理し (ステップ S 518)、貸出元のライセンス管理情報から貸出時のライセンス ID を取得する (ステップ S 520)。そして、コントローラ 40 は、取得したライセンス ID と、ステップ S 518 において受理した暗号化データ {K s 2 a} K m 3 とを 1 つにデータにしてライセンス ID / / {K s 2 a} K m 3 をメモリカード 110 へ送信する (ステップ S 522)。そうすると、メモリカード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424、およびバス B S 4 を介してライセンス ID / / {K s 2 a} K m 3 を受理する (ステップ S 524)。その後、コントローラ 1420 は、暗号化データ {K s 2 a} K m 3 を復号処理部 1422 へ与え、復号処理部 1422 は、K m 保持部

1421 からのクラス秘密復号鍵 K m 3 によって {K s 2 a} K m 3 を復号してセッションキー K s 2 a を受理する (ステップ S 526)。そして、セッションキー発生部 1418 は、セッションキー K s 2 b を生成し (ステップ S 528)、暗号化処理部 1406 は、切換スイッチ 1446 の端子を順次切換えることによって取得したセッションキー K s 2 b、および個別公開暗号鍵 K P m c 4 を、復号処理部 1404 によって復号されたセッションキー K s 2 a によって暗号化し、暗号化データ {K s 2 b / / K P m c 4} K s 2 a を生成する。コントローラ 1420 は、暗号化データ {K s 2 b / / K P m c 4} K s 2 a をバス B S 4、インタフェース 1424 および端子 1426 を介して出力し (ステップ S 530)、コントローラ 510 は、端子 580 および USB インタフェース 550 を介して暗号化データ {K s 2 b / / K P m c 4} K s 2 a を受理する。そして、コントローラ 510 は、暗号化データ {K s 2 b / / K P m c 4} K s 2 a をバス B S 2 を介してライセンス管理デバイス 520 へ送信する (ステップ S 532)。

【0199】そうすると、ライセンス管理デバイス 520 のコントローラ 5220 は、端子 5226、インタフェース 5224 およびバス B S 5 を介して暗号化データ {K s 2 b / / K P m c 4} K s 2 a を受信し、その受信した暗号化データ {K s 2 b / / K P m c 4} K s 2 a を復号処理部 5212 に与える。復号処理部 5212 は、セッションキー発生部 5218 からのセッションキー K s 2 a によって暗号化データ {K s 2 b / / K P m c 4} K s 2 a を復号し、セッションキー K s 2 b、および公開暗号鍵 K P m c 4 を受理する (ステップ S 534)。

【0200】そして、コントローラ 510 は、ライセンスの検索要求を貸出先のメモリカード 110 へ入力する (ステップ S 534)。メモリカード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424 およびバス B S 4 を介してライセンスの検索要求を受理し (ステップ S 536)、ステップ S 524 において受理したライセンス ID に基づいてメモリ 1415 のライセンス領域 1415 A を検索する。そして、コントローラ 1420 は、検索結果 s t a t e を生成する (ステップ S 538)。

【0201】暗号化処理部 1406 は、復号処理部 1412 によって復号して得られたセッションキー K s 2 a をスイッチ 1442 の接点 P b を介して受け、セッションキー発生部 1418 が発生したセッションキー K s 2 b をスイッチ 1446 の接点 P d を介して受ける。そして、暗号化処理部 1406 は、セッションキー K s 2 b をセッションキー K s 2 a によって暗号化して暗号化データ {K s 2 b} K s 2 a を生成する (ステップ S 540)。そして、コントローラ 1420 は、ライセンス ID / / {K s 2 b} K s 2 a / / s t a t e を生成し、

その生成したライセンスID// {Ks 2 b} Ks 2 a // state のハッシュ値 hash を求める (ステップ S 5 4 2)。つまり、コントローラ 1 4 2 0 は、ライセンスID// {Ks 2 b} Ks 2 a // state の署名を行なう。その後、コントローラ 1 4 2 0 は、ハッシュ値 hash をスイッチ 1 4 4 6 の接点 Pf を介して暗号化処理部 1 4 0 6 へ与える。暗号化処理部 1 4 0 6 は、ハッシュ値 hash をセッションキー Ks 2 a によって暗号化し、暗号化データ {hash} Ks 2 a を生成する (ステップ S 5 4 4)。

【0202】図 19 を参照して、メモリカード 1 1 0 のコントローラ 1 4 2 0 は、ライセンスID// {Ks 2 b} Ks 2 a // state // {hash} Ks 2 a を生成し、バス BS 4、インタフェース 1 4 2 4、および端子 1 4 2 6 を介してライセンスID// {Ks 2 b} Ks 2 a // state // {hash} Ks 2 a を出力する (ステップ S 5 4 6)。コントローラ 5 1 0 は、端子 5 8 0 および USB インタフェース 5 5 0 を介してメモリカード 1 1 0 からライセンスID// {Ks 2 b} Ks 2 a // state // {hash} Ks 2 a を受信する (ステップ S 5 4 8)。そして、コントローラ 5 1 0 は、貸出元のライセンス管理情報から返却するライセンスが格納されているエントリ番号を取得し

(ステップ S 5 5 0)、ステップ S 5 4 8 において取得したライセンスID// {Ks 2 b} Ks 2 a // state // {hash} Ks 2 a とエントリ番号を指定したライセンス返却要求とを貸出元のライセンス管理デバイス 5 2 0 へ入力する (ステップ S 5 5 2)。ライセンス管理デバイス 5 2 0 のコントローラ 5 2 2 0 は、端子 5 2 2 6、インタフェース 5 2 2 4 およびバス BS 5 を介してライセンスID// {Ks 2 b} Ks 2 a // state // {hash} Ks 2 a とエントリ番号とライセンス返却要求とを受理し (ステップ S 5 5 4)、その受理したエントリ番号によって指定された領域に格納されている貸出フラグ、貸出時のライセンスID、および貸出先IDに格納された公開暗号鍵 K P m c x を取得する (ステップ S 5 5 6)。

【0203】そうすると、コントローラ 5 2 2 0 は、取得した公開暗号鍵 K P m c x がステップ S 5 3 4 において受理したメモリカード 1 1 0 に固有の公開暗号鍵 K P m c 4 に一致するか否かを判定し (ステップ S 5 5 8)、不一致であるとき、返却動作は終了する (ステップ S 6 3 8)。つまり、メモリカード 1 1 0 がライセンスを貸出した相手でないことが判定されたことになるので、返却動作を終了することにしたものである。公開暗号鍵 K P m c x が公開暗号鍵 K P m c 4 に一致したとき、コントローラ 5 2 2 0 は、貸出フラグが貸出中になっているか否かを判定し (ステップ S 5 6 0)、貸出中でなければライセンスを返却する必要がないので、返却動作は終了する (ステップ S 6 3 8)。ステップ S 5 6 0 にお

いてライセンスが返却中であると判定されると、コントローラ 5 2 2 0 は、受理したライセンスIDが貸出時のライセンスIDに一致するか否かを判定し (ステップ S 5 6 2)、不一致であるとき、返却動作は終了する (ステップ S 6 3 8)。つまり、返却要求のあったライセンスのライセンスIDが貸出したライセンスのライセンスIDに一致せず、貸出したライセンスが返却されないことになるので、返却動作を終了することにしたものである。ステップ S 5 6 2 において、2 つのライセンスIDが一致したとき、コントローラ 5 2 2 0 は、メモリカード 1 1 0 におけるライセンスの検索結果 state を確認する (ステップ S 5 6 4)。すなわち、コントローラ 5 2 2 0 は、返却しようとするライセンスがメモリカード 1 1 0 のライセンス領域 1 4 1 5 A に本当に格納されているか否かを確認し、ライセンス領域 1 4 1 5 A に格納されていないとき、返却動作を終了する (ステップ S 6 3 8)。そして、コントローラ 5 2 2 0 は、返却しようとするライセンスがメモリカード 1 1 0 のライセンス領域 1 4 1 5 A に格納されていることを確認したとき、ライセンスID// {Ks 2 b} Ks 2 a // state のハッシュ値 hash を求める (ステップ S 5 6 6)。つまり、ライセンス管理デバイス 5 2 0 のコントローラ 5 2 2 0 は、自らライセンスID// {Ks 2 b} Ks 2 a // state に対する署名を行ない、ハッシュ値 hash を求める。

【0204】その後、コントローラ 5 2 2 0 は、ステップ S 5 5 4 において受理した {hash} Ks 2 a を復号処理部 5 2 1 2 に与える。復号処理部 5 2 1 2 は、

{hash} Ks 2 a をセッションキー Ks 2 a によって復号し、コントローラ 5 2 2 0 は、メモリカード 1 1 0 におけるハッシュ値 hash を受理する (ステップ S 5 6 8)。そして、コントローラ 5 2 2 0 は、自ら求めたハッシュ値 hash がメモリカード 1 1 0 におけるハッシュ値 hash に一致するか否かを判定し (ステップ S 5 7 0)、不一致であるとき、メモリカード 1 1 0 における署名が書換えられていることになるので返却動作は終了する (ステップ S 6 3 8)。2 つのハッシュ値が一致したとき、コントローラ 5 2 2 0 は、ステップ S 5 5 4 において受理した暗号化データ {Ks 2 b} Ks 2 a を復号処理部 5 2 1 2 に与える。復号処理部 5 2 1 2 は、暗号化データ {Ks 2 b} Ks 2 a をセッションキー Ks 2 a によって復号してセッションキー Ks 2 b を受理する (ステップ S 5 7 2)。

【0205】そして、コントローラ 5 2 2 0 は、セッションキー Ks 2 b の確認を行ない (ステップ S 5 7 4)、ライセンスの貸出時にメモリカード 1 1 0 から受信したセッションキー Ks 2 b と不一致であれば返却動作は終了し (ステップ S 6 3 8)、一致すれば図 20 のステップ S 5 7 6 へ移行する。

【0206】図 20 を参照して、貸出先に貸出したライ



センスを無効にするための無効ダミーライセンス（偽ライセンスID、偽コンテンツID、偽ライセンス鍵Kc、偽アクセス制御情報ACm、および偽再生制御情報ACp）を生成し、その生成した無効ダミーライセンスを暗号化処理部5217に与える。暗号化処理部5217は、無効ダミーライセンスを復号処理部5212によって復号された公開暗号鍵Kpmc4によって暗号化し、暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4を生成する（ステップS576）。そして、暗号化処理部5206は、暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4をスイッチ5246の接点Pcを介して受取り、その受取った暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4をスイッチ5246の接点Pdを介して受取ったセッションキーKs2bによって暗号化して暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4}Ks2bを出力する。そして、コントローラ5220は、バスBS5、インタフェース5224、および端子5226を介して暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4}Ks2bを出力する（ステップS578）。

【0207】コントローラ510は、バスBS2を介して暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4}Ks2bを貸出元であるライセンス管理デバイス520から受け、貸出先であるメモリカード110へ暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4}Ks2bを送信する（ステップS580）。

【0208】メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4}Ks2bを受信し、その受信した暗号化データを復号処理部1412に与える。復号処理部1412は、暗号化データをセッションキーKs2bによって復号して{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4を受信する（ステップS582）。そして、復号処理部1404は、復号処理部14

12からの暗号化データ{偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp}Kmc4をKmc保持部1402からの秘密鍵Kmc4によって復号して無効ダミーライセンス（偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp）を受信する（ステップS584）。

【0209】そうすると、コントローラ510は、貸出先であるメモリカード110のライセンス管理情報から返却するライセンスが格納されているエントリ番号を取得し、その取得したエントリ番号を貸出先に送信する（ステップS586）。メモリカード110のコントローラ1420は、偽アクセス制御ACmによってライセンスの貸出が可能か否かを判定し（ステップS588）、貸出可であればライセンス領域の貸出フラグを「可」に設定し（ステップS590）、貸出不可であれば貸出フラグを「不可」に設定する（ステップS592）。ステップS590またはステップS592の後、コントローラ1420は、エントリ番号によって指定されたライセンス領域1415Aの有効フラグを「有効」に設定し（ステップS694）、エントリ番号によって指定された領域にライセンス（ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報、および再生回数制御情報）を格納する（ステップS596）。ステップS588、S590、S592、S594、S596の処理は、上述した「配信」および「移動」と共通としているため、処理されるものの偽アクセス制御情報ACmは、常に移動複製禁止であるためステップS588においては必ず「貸出不可」と判断され、ステップS592に進む。

【0210】その後、コントローラ510は、ライセンスの検索要求を貸出先に再び入力し（ステップS598）、メモリカード110のコントローラ1420は、ライセンスの検索結果を端子1426、インタフェース1424、およびバスBS4を介して受信する（ステップS600）。コントローラ1420は、ライセンスIDに基づいてメモリ1415のライセンス領域1415Aを検索する。そして、コントローラ1420は、検索結果stateを生成する（ステップS602）。

【0211】暗号化処理部1406は、復号処理部1412によって復号して得られたセッションキーKs2aをスイッチ1442の接点Pbを介して受け、セッションキー発生部1418が発生したセッションキーKs2bをスイッチ1446の接点Pdを介して受ける。そして、暗号化処理部1406は、セッションキーKs2bをセッションキーKs2aによって暗号化して暗号化データ{Ks2b}Ks2aを生成する（ステップS604）。そして、コントローラ1420は、ライセンスID//{Ks2b}Ks2a//stateを生成し、

その生成したライセンスID//{Ks2b}Ks2a//stateのハッシュ値hashを求める(ステップS606)。つまり、コントローラ1420は、ライセンスID//{Ks2b}Ks2a//stateの署名を行なう。その後、コントローラ1420は、ハッシュ値hashをスイッチ1446の接点Pfを介して暗号化処理部1406へ与える。暗号化処理部1406は、ハッシュ値hashをセッションキーKs2aによって暗号化し、暗号化データ{hash}Ks2aを生成する(ステップS608)。

【0212】図21を参照して、メモリカード110のコントローラ1420は、ライセンスID//{Ks2b}Ks2a//state//{hash}Ks2aを生成し、バスBS4、インタフェース1424、および端子1426を介してライセンスID//{Ks2b}Ks2a//state//{hash}Ks2aを出力する(ステップS610)。コントローラ510は、端子580、USBインタフェース550を介してメモリカード110からライセンスID//{Ks2b}Ks2a//state//{hash}Ks2aを受信する(ステップS612)。そして、コントローラ510は、ライセンスID//{Ks2b}Ks2a//state//{hash}Ks2aとエントリ番号を指定したライセンス返却確認要求とをバスBS2を介して貸出元であるライセンス管理デバイス520へ入力する(ステップS614)。

【0213】ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS2を介してライセンスID//{Ks2b}Ks2a//state//{hash}Ks2aとエントリ番号とライセンス返却確認要求とを受信する(ステップS616)。そして、コントローラ5220は、受理したライセンスIDが貸出時のライセンスIDに一致するか否かを判定し(ステップS618)、不一致であれば返却動作は終了する(ステップS638)。そして、ステップS618において、2つのライセンスIDが一致すると判定されたとき、コントローラ5220は、メモリカード110におけるライセンスの検索結果stateを確認する(ステップS620)。すなわち、コントローラ5220は、返却しようとするライセンスがメモリカード110のライセンス領域1415Aから本当に消去されているか否かを確認し、ライセンス領域1415Aにライセンスが存在するとき、返却動作を終了する(ステップS638)。そして、コントローラ5220は、返却しようとするライセンスがメモリカード110のライセンス領域1415Aから消去されていることを確認したとき、ライセンスID//{Ks2b}Ks2a//stateのハッシュ値hashを求める(ステップS622)。つまり、ライセンス管理デバイス520のコントローラ5220は、自ら

ライセンスID//{Ks2b}Ks2a//stateに対する署名を行ない、ハッシュ値hashを求める。

【0214】その後、コントローラ5220は、ステップS554において受理した{hash}Ks2aを復号処理部5212に与える。復号処理部5212は、{hash}Ks2aをセッションキーKs2aによって復号し、コントローラ5220は、メモリカード110におけるハッシュ値hashを受信する(ステップS624)。そして、コントローラ5220は、自ら求めたハッシュ値hashがメモリカード110におけるハッシュ値hashに一致するか否かを判定し(ステップS626)、不一致であるとき、メモリカード110における署名が書換えられていることになるので返却動作は終了する(ステップS638)。2つのハッシュ値が一致したとき、コントローラ5220は、ステップS616において受理した暗号化データ{Ks2b}Ks2aを復号処理部5212に与える。復号処理部5212は、暗号化データ{Ks2b}Ks2aをセッションキーKs2aによって復号してセッションキーKs2bを受信する(ステップS628)。

【0215】そして、コントローラ5220は、セッションキーKs2bの確認を行ない(ステップS630)、ライセンスの貸出時にメモリカード110から受信したセッションキーKs2bと不一致であれば返却動作は終了する(ステップS638)。ステップS630において2つのセッションキーKs2bが一致したとき、コントローラ1420は、エントリ番号によって指定されたエントリ内の貸出フラグを「可」に変更する(ステップS632)。そして、コントローラ40は、返却したライセンスの情報を削除し、貸出先のメモリカード110のデータ領域1415Bに記録されているライセンス管理情報および再生リストファイルを更新し、返却動作が終了する(ステップS638)。

【0216】このように、暗号化コンテンツデータおよびライセンスを貸出した相手先から暗号化コンテンツデータおよびライセンスを返却して貰うことによって、ライセンス管理デバイス520にライセンスを残したまま、携帯電話機100および再生端末102において暗号化コンテンツデータを再生して楽しむことができる。

【0217】また、メモリカードへ貸出されたライセンスは、アクセス制御情報ACmによってメモリカードから他の記録機器(メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール)に対して、チェックアウトしたライセンスが出力できないよう指定されているため、貸出したライセンスが流出することはない。貸出したライセンス管理モジュールに対してチェックイン(返却)することで、貸出したライセンスの権利が、貸出したライセンス管理デバイスに戻るようになっている。したがって、著作者の意に反して複製ができること

を許すものではなく、セキュリティレベルが低下する処理ではなく、著作権も保護されている。

【0218】図22を参照して、パーソナルコンピュータ50のライセンス管理モジュール511またはライセンス管理デバイス520によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ50のHDD530は、コンテンツリストファイル150と、コンテンツファイル1531~1535と、ライセンス管理ファイル1521~1525とを含む。

【0219】コンテンツリストファイル150は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報（楽曲名、アーティスト名など）と、コンテンツファイルとライセンス管理ファイルとを示す情報（ファイル名）などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Dc-infから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、ライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

【0220】コンテンツファイル1531~1535は、ライセンス管理モジュール511またはライセンス管理デバイス520によって受信された暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを記録するファイルであり、コンテンツごとに設けられる。

【0221】また、ライセンス管理ファイル1521~1525は、それぞれ、コンテンツファイル1531~1535に対応して記録されており、ライセンス管理モジュール511またはライセンス管理デバイス520によって受信されたライセンスを管理するためのファイルである。これまでの説明でも明らかなように、ライセンスは通常参照することができないが、ライセンス鍵Kcを除く他の情報は、ユーザが書き換えることさえできなければ著作権保護の点では問題ない。しかし、運用においてライセンス鍵Kcと分離して管理することはセキュリティの低下につながるため好ましくない。そこで、ライセンス配信を受ける場合に平文にて参照できるトランザクションID、コンテンツIDや、ライセンス購入条件ACから容易に判断できるアクセス制御情報ACmおよび再生制御情報ACpにて制限されている事項の写しおよびチェックアウトの記録を平文にて記録する。さらに、ライセンス管理デバイス520にライセンスが記録された場合にはエントリ番号を記録する。

【0222】ライセンス管理ファイル1521, 1522, 1524, 1525は、それぞれ、エントリ番号0, 2, 1, 3を含む。これは、ライセンス管理デバイス520によって受信され、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Aにおいて管理されるライセンス（ライセンスID、ライセン

ス鍵Kc、アクセス制御情報ACmおよび再生制御情報ACm）の管理領域を指定する番号である。

【0223】また、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを携帯電話機100または再生端末102に装着されたメモリカード110へ移動させるとき、コンテンツファイル1531~1535を検索してコンテンツファイル1531を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル1531に対応するライセンス管理ファイル1521に含まれるエントリ番号は「0」であるので、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Aのエントリ番号0によって指定された領域に記録されている。そうすると、HDD530に記録されたコンテンツリストファイル150のライセンス管理ファイル1521からエントリ番号0を読み出し、その読み出したエントリ番号0をライセンス管理デバイス520に入力することによって、メモリ5215のライセンス領域5215Aからライセンスを容易に取出し、メモリカード110へ移動できる。そして、ライセンスを移動した後は、メモリ5215のライセンス領域5215Aにおいて指定されたエントリ番号内の有効フラグが「無効」にされるので（図15のステップS346参照）、それに対応してライセンス管理ファイル1523のように「ライセンス無」が記録される。

【0224】ライセンス管理ファイル1523は、「ライセンス無」を含む。これは、ライセンス管理デバイス520によって受信されたライセンスが、移動された結果である。対応するコンテンツファイル1533はHDD530に記録されたままになっている。メモリカードからライセンスを再びライセンス管理モジュール520へ移動、あるいは、配信サーバ10から再び配信を受ける場合には、ライセンスについてのみ配信を受けることが可能である。

【0225】貸出および返却においても、同様にエントリ番号を指定して処理することができる。また、貸出においては、ライセンス管理ファイルは、貸出の有無および貸出先を特定するための情報、たとえば、メモリカードに割当てられたメディアID等および貸出時のライセンスIDを記録する。これらの情報は、返却時に消去される。

【0226】このように、本発明においては、ライセンス管理デバイス520に記録されているライセンスをライセンス管理デバイス520に残したまま、セキュリティレベルを低下させることなく、著作権を保護しながら暗号化コンテンツデータの再生を携帯電話機100や再生端末102によって自由に行なうことができる。

【0227】図23は、メモリカード110のメモリ1

415におけるライセンス領域1415Aとデータ領域1415Bとを示したものである。データ領域1415Bには、再生リストファイル160とコンテンツファイル1611~161nと、ライセンス管理ファイル1621~162nとが記録されている。コンテンツファイル1611~161nは、受信した暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを1つのファイルとして記録する。また、ライセンス管理ファイル1621~162nは、それぞれ、コンテンツファイル1611~161nに対応して記録されている。パーソナルコンピュータ50におけるHDD530に記録されていた各データがメモリカード110のメモリ1415のデータ領域1415Bに記録されているのみで、他の点は、図22と同じである。

【0228】また、ライセンス管理ファイル1622は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル1612は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、再生端末が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

【0229】また、コンテンツファイル1613は、点線で示されているが、これは、たとえば、再生端末が配信サーバ10から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータをパーソナルコンピュータ50へ送信した場合に相当し、ライセンスはメモリ1415に存在するが暗号化コンテンツデータが存在しないことを意味する。

【0230】なお、ライセンス管理領域1415Aは、ライセンス管理デバイスのライセンス管理領域5215Aと同じ構成になっている。したがって、メモリカード110から他のメモリカードへの貸出し、さらにはライセンス管理デバイス520への貸出しも可能である。

【0231】〔再生〕上述したように、携帯電話機100または再生端末102に装着されたメモリカード110は、配信サーバ10から、直接、暗号化コンテンツデータおよびライセンスを受信できる。また、メモリカード110は、パーソナルコンピュータ50が配信サーバ10からハード的に取得した暗号化コンテンツデータおよびライセンスを、「移動」という概念によってパーソナルコンピュータ50から受信できる。さらに、メモリカード110は、パーソナルコンピュータ50が配信サーバ10または音楽CDからソフト的に取得した暗号化コンテンツデータおよびライセンスを、「貸出」という概念によってパーソナルコンピュータ50から受信できる。

【0232】このように、メモリカード110は、各種の方法によって暗号化コンテンツデータおよびライセンスを受信する。そこで、次に、これらの各種の方法によってメモリカードが受信した暗号化コンテンツデータの

再生について説明する。

【0233】図24は、メモリカード110が受信したコンテンツデータの再生端末102における再生動作を説明するためのフローチャートである。なお、図24における処理以前に、再生端末102のユーザは、メモリカード100のデータ領域1415Bに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【0234】図24を参照して、再生動作の開始とともに、再生端末100のユーザから操作パネル1108を介して再生リクエストが再生端末100にインプットされる（ステップS700）。そうすると、コントローラ1106は、バスBS3を介して認証データの出力要求をコンテンツ再生回路1550に行ない（ステップS702）、コンテンツ再生回路1550は認証データの出力要求を受信する（ステップS704）。そして、認証データ保持部1500は、認証データ{Kpp1/Cp1}KPaを出力し（ステップS706）、コントローラ1106は、メモリカードインタフェース1200を介してメモリカード110へ認証データ{Kpp1/Cp1}KPaを入力する（ステップS708）。

【0235】そうすると、メモリカード110は、認証データ{Kpp1/Cp1}KPaを受信し、復号処理部1408は、受信した認証データ{Kpp1/Cp1}KPaを、KPa保持部1414に保持された公開認証鍵KPaによって復号し（ステップS710）、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{Kpp1/Cp1}KPaが正規の認証データであるか否かを判断する認証処理を行なう（ステップS712）。復号できなかった場合、ステップS748へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ1420は、セッションキー発生部1418を制御し、セッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる（ステップS714）。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kpp1によって暗号化した{Ks2}Kp1をバスBS3へ出力する。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ{Ks2}Kp1を出力する（ステップS716）。再生端末100のコントローラ1106は、メモリカードインタフェース1200を介して{Ks2}Kp1を取得する。そして、コントローラ1106は、{Ks2}Kp1をバスBS3を介してコンテンツ再生回路1550の復号処理部1504へ与え（ステップS718）、復号処理部1504は、Kp1保持部1502から出力された、公開

暗号鍵Kp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号処理部1506へ出力する(ステップS720)。そうすると、セッションキー発生部1508は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1506へ出力する(ステップS722)。暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3を復号処理部1504からのセッションキーKs2によって暗号化して{Ks3}Ks2を出力し(ステップS724)、コントローラ1106は、バスBS3およびメモリカードインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する(ステップS726)。

【0236】そうすると、メモリカード110の復号処理部1412は、端子1426、インタフェース1424、およびバスBS4を介して{Ks3}Ks2を入力する。復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、再生端末100で発生されたセッションキーKs3を受理する(ステップS728)。

【0237】再生端末のコントローラ1106は、メモリカード110から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し(ステップS730)、メモリカードインタフェース1200を介してメモリカード110へ取得したエントリ番号とライセンスの出力要求を出力する(ステップS732)。

【0238】メモリカード110のコントローラ1420は、エントリ番号とライセンスの出力要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスを取得する(ステップS734)。

【0239】そして、コントローラ1420は、アクセス制限情報ACmを確認する(ステップS736)。

【0240】ステップS736においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ACmを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ACmの再生回数を変更した(ステップS738)後に次のステップ(ステップS740)に進む。一方、アクセス制限情報ACmの再生回数によって再生が制限されていない場合には、ステップS738はスキップされ、アクセス制限情報ACmの再生回数は変更されることなく処理が次のステップ(ステップS740)に進行される。

【0241】ステップS736において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415Aに記録された再

生リクエスト曲のライセンス鍵Kcおよび再生制御情報ACpがバスBS4上へ出力される(ステップS740)。

【0242】得られたライセンス鍵Kcと再生制御情報ACpは、切換スイッチ1446の接点Pfを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点Pbを介して復号処理部1412より受けたセッションキーKs3によって切換スイッチ1446を介して受けたライセンス鍵Kcと再生制御情報ACpとを暗号化し、{Kc//ACp}Ks3をバスBS4へ出力する(ステップS740)。

【0243】バスBS4へ出力された暗号化データは、インタフェース1424、端子1426、およびメモリカードインタフェース1200を介して再生端末102に送出される。

【0244】再生端末102においては、メモリカードインタフェース1200を介してバスBS3に伝達される暗号化データ{Kc//ACp}Ks3を復号処理部1510によって復号処理を行ない、ライセンス鍵Kcおよび再生制御情報ACpを受理する(ステップS742、S744)。復号処理部1510は、ライセンス鍵Kcを復号処理部1516に伝達し、再生制御情報ACpをバスBS3へ出力する。

【0245】コントローラ1106は、バスBS3を介して、再生制御情報ACpを受理して再生の可否の確認を行なう(ステップS746)。

【0246】ステップS746においては、再生制御情報ACpによって再生不可と判断される場合には、再生動作は終了される。

【0247】ステップS746において再生可能と判断された場合、コントローラ1106は、メモリカードインタフェース1200を介してメモリカード110に暗号化コンテンツデータ{Dc}Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Dc}Kcを取得し、バスBS4、インタフェース1424、および端子1426を介してメモリカードインタフェース1200へ出力する。

【0248】再生端末102のコントローラ1106は、メモリカードインタフェース1200を介して暗号化コンテンツデータ{Dc}Kcを取得し、バスBS3を介して暗号化コンテンツデータ{Dc}Kcをコンテンツ再生回路1550へ与える。

【0249】そして、コンテンツ再生回路1550の復号処理部1516は、暗号化コンテンツデータ{Dc}Kcを復号処理部1510から出力されたライセンス鍵Kcによって復号してコンテンツデータDcを取得する。

【0250】そして、復号されたコンテンツデータDcは音楽再生部1518へ出力され、音楽再生部1518

は、コンテンツデータを再生し、DA変換器1519はデジタル信号をアナログ信号に変換して端子1530へ出力する。そして、音楽データは端子1530から外部出力装置を介してヘッドホーン130へ出力されて再生される。これによって再生動作が終了する（ステップS748）。

【0251】本発明の実施の形態によれば、貸出元のメモリカードは、貸出したライセンスを貸出先IDおよび貸出時ライセンスIDによって管理し、ライセンスの貸出を貸出フラグによって管理し、ライセンスの貸出時に貸出用ライセンスを自己が保持したライセンスから生成し、元のライセンスが貸出中であることを示すフラグを貸出フラグに設定するので、貸出したライセンスのバックアップを提供することができる。

【0252】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0253】

【発明の効果】本発明によれば、貸出元のメモリカードは、貸出したライセンスを貸出先IDおよび貸出時ライセンスIDによって管理し、ライセンスの貸出を貸出フラグによって管理し、ライセンスの貸出時に貸出用ライセンスを自己が保持したライセンスから生成し、元のライセンスが貸出中であることを示すフラグを貸出フラグに設定するので、貸出したライセンスのバックアップを提供することができる。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 他のデータ配信システムを概念的に説明する概略図である。

【図3】 図1および図2に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1および図2に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 図1および図2に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図6】 図1および図2に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図である。

【図7】 図2に示すデータ配信システムにおける再生端末の構成を示す概略ブロック図である。

【図8】 図1および図2に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図9】 図6に示すライセンス管理デバイスの構成を示す概略ブロック図である。

【図10】 図1および図2に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図11】 図1および図2に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図12】 リッピングを実行するソフトウェアの機能を説明するための機能ブロック図である。

【図13】 図1および図2に示すデータ配信システムにおけるリッピングの動作を説明するためのフローチャートである。

【図14】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第1のフローチャートである。

【図15】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第2のフローチャートである。

【図16】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの貸出動作を説明するための第1のフローチャートである。

【図17】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの貸出動作を説明するための第2のフローチャートである。

【図18】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第1のフローチャートである。

【図19】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第2のフローチャートである。

【図20】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第3のフローチャートである。

【図21】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第4のフローチャートである。

【図22】 パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

【図23】 メモリカードにおける再生リストファイルの構成を示す図である。

【図24】 再生端末における再生動作を説明するためのフローチャートである。

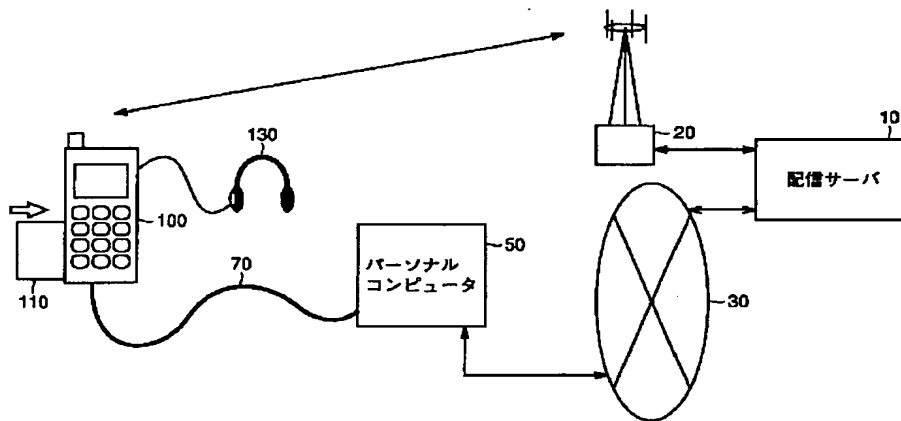
【符号の説明】

10 配信サーバ、20 配信キャリア、30 インターネット網、50 パーソナルコンピュータ、60 音楽CD、70 USBケーブル、100 携帯電話機、102 再生端末、110 メモリカード、130 ヘッドホーン、150 コンテンツリストファイル、16

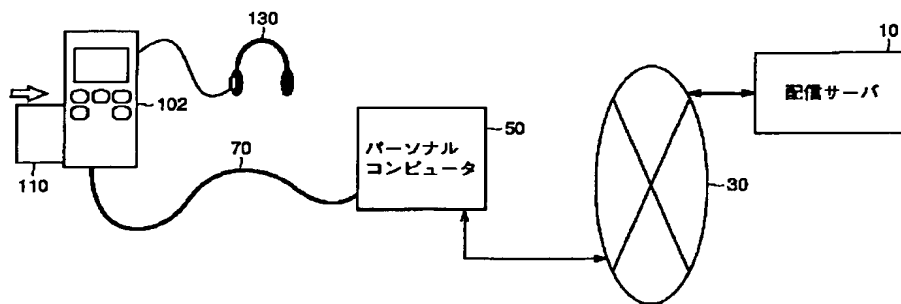
0 再生リストファイル、302 課金データベース、304 情報データベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1404、1408、1412、1422、1504、1510、1516、5204、5208、5212、5222 復号処理部、313 認証鍵保持部、315 配信制御部、316、セッションキー発生部、318、326、328、1406、1410、1417、1506、5206、5210、5217、5405 暗号処理部、350 通信装置、510、1106、1420、5220 コントローラ、520 ライセンス管理デバイス、530 ハードディスク、550、1112 USBインタフェース、555 モデム、560 キーボード、570 ディスプレイ、580、1114、1426、1530、5226 端子、1108 操作パネル、1110 表示パネル、1200 メモリカードインタフェース、140

0、1500、5200 認証データ保持部、1402、5202 Kmc保持部、1414、5214 KPa保持部、1415、5215 メモリ、1415A ライセンス領域、1415B データ領域、1416、5216 KPmc保持部、1418、5218 セッションキー発生部、1421、5221 Km保持部、1424、5224 インタフェース、1442、1446、5242、5246 切換スイッチ、1502 Kp1保持部、1518 音楽再生部、1519 DA変換器、1521～1525、1621～162n ライセンス管理ファイル、1531～1535、1611～161n コンテンツファイル、1550 コンテンツ再生回路、5400 ウォータマーク検出手段、5401 ウォータマーク判定手段、5402 リマーク手段、5403 ライセンス発生手段、5404 音楽エンコーダ。

【図1】



【図2】



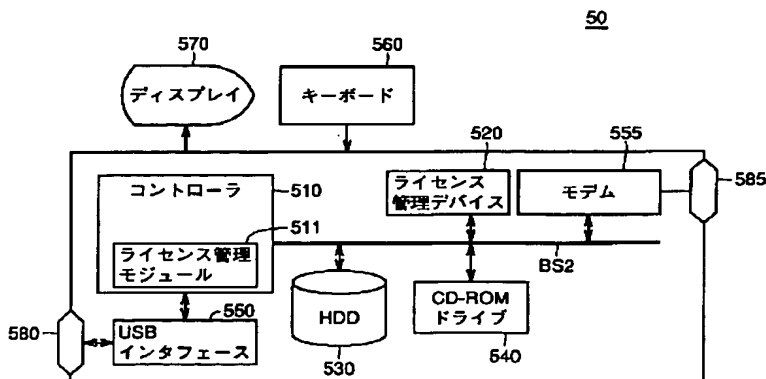
【図3】

| 記号         | 種類       | 属性       | 特性  |
|------------|----------|----------|---|
| Dc         | コンテンツデータ | コンテンツ固有  | 例：音楽データ、朗読データ、教材データ、画像データ<br>Kcにて復号可能な暗号化コンテンツデータ<br>(Dc)Kcとして配信され、メモ리카ードに保持される |
| Dc-Inf     | 付加情報     | コンテンツ固有  | Dcに付随する平文データ。   |
| Kc         | ライセンス    | コンテンツ固有  | ライセンス<br>暗号化コンテンツデータを復号する復号鍵  |
| ACm/ACp    | ライセンス    | ライセンス固有  | 制限情報<br>再生やライセンスの取り扱いに対する制限事項   |
| コンテンツID    | ライセンス    | コンテンツ固有  | コンテンツを特定するための管理コード  |
| ライセンスID    | ライセンス    | ライセンス固有  | ライセンスを特定するための管理コード  |
| ライセンス      | ライセンス    | ライセンス固有  | Kc+ACm+ACp+コンテンツID+ライセンスIDの総称   |
| 有効フラグ      | フラグ      | ライセンス固有  | ライセンスをメモ리카ードから外部へ出すことが可能か否かを表す。   |
| 貸出フラグ      | フラグ      | ライセンス固有  | ライセンスの貸出の可否を表す。   |
| 貸出先ID      | 特定情報     | メモ리카ード固有 | ライセンスを貸出した貸出先を特定するための情報   |
| 貸出時ライセンスID | 識別情報     | ライセンス固有  | 貸出したライセンスを識別するための情報   |

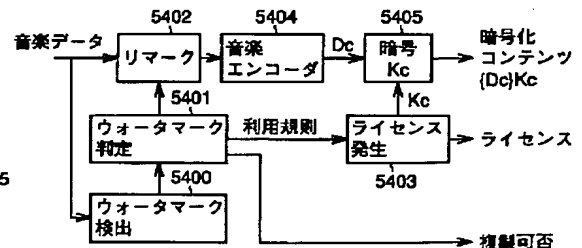
【図4】

|             | 記号    | 種類     | 属性      | 特性   |
|-------------|-------|--------|---------|--|
| 配信サーバ       | KPa   | 公開鍵暗号鍵 | システム共通  | 認証局にて認証データを復号する鍵   |
|             | Ka1   | 共通鍵    | セッション固有 | メモ리카ード、ライセンス管理デバイスへのライセンス配信ごとに発生   |
| メモ리카ード      | KPa   | 公開鍵暗号鍵 | システム共通  | 認証局にて認証データを復号する鍵<br>配信サーバのKPaと同一   |
| ライセンス管理デバイス | KPmw  | 公開暗号鍵  | クラス固有   | 証明書Cmwとともに認証局にて暗号化された認証データとして保持<br>wはクラスを識別するための識別子  |
|             | Kmw   | 秘密復号鍵  | クラス固有   | 公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵   |
|             | KPmax | 公開暗号鍵  | 個別      | メモ리카ードごとに異なる。<br>xはモジュールを識別するための識別子  |
|             | Kmx   | 秘密復号鍵  | 個別      | 公開暗号鍵KPmaxにて暗号化されたデータを復号する非対称な復号鍵  |
|             | Ka2   | 共通鍵    | セッション固有 | ライセンスの授受ごとに発生  |
|             | Cmw   | 証明書    | クラス証明書  | メモ리카ード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。暗証機能を有する。<br>[KPmw/Cmw]KPaの形式で出荷時に記録。<br>*メモ리카ードおよびライセンス管理デバイスのクラスwごとに異なる。 |
| コンテンツ再生回路   | KPpy  | 公開暗号鍵  | クラス固有   | 証明書Cmwとともに認証局にて暗号化された認証データとして保持<br>yはクラスを識別するための識別子  |
|             | Kpy   | 秘密復号鍵  | クラス固有   | 公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵   |
|             | Ka3   | 共通鍵    | セッション固有 | 配信サーバまたは音楽再生モジュール間の再生セッションごとに発生  |
|             | Cpy   | 証明書    | クラス証明書  | コンテンツ再生回路のクラス証明書。暗証機能を有する。<br>[KPpy/Cpy]KPaの形式で出荷時に記録。<br>*コンテンツ再生回路のクラスyごとに異なる。                                     |

【図6】

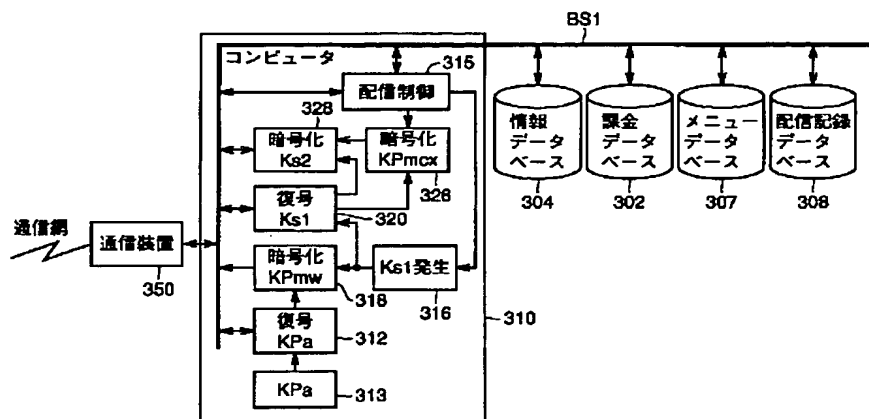


【図12】

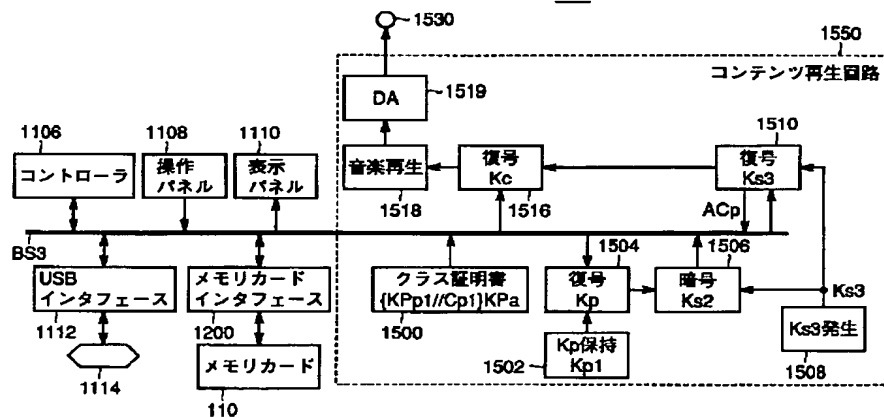




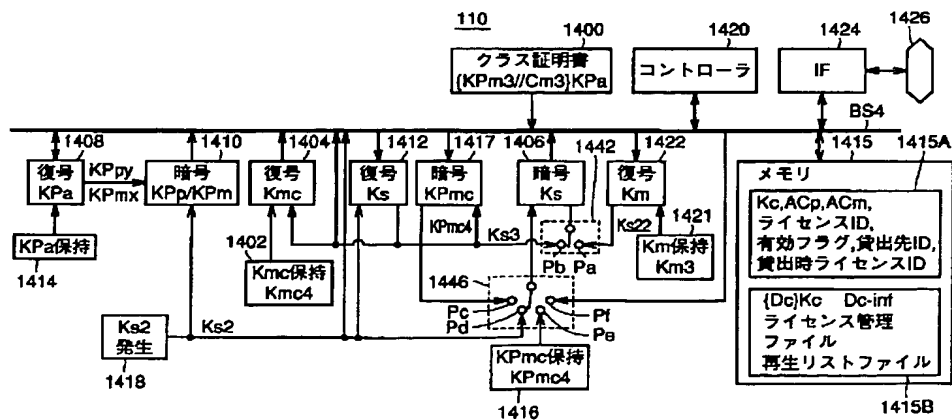
10



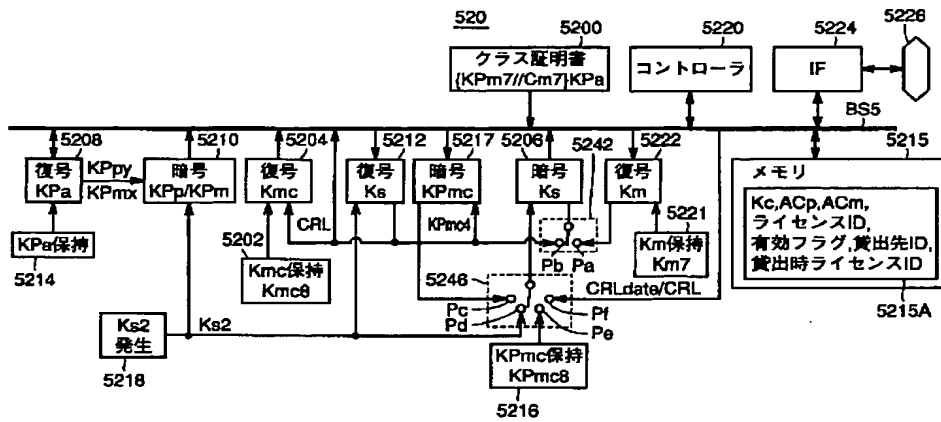
**102**



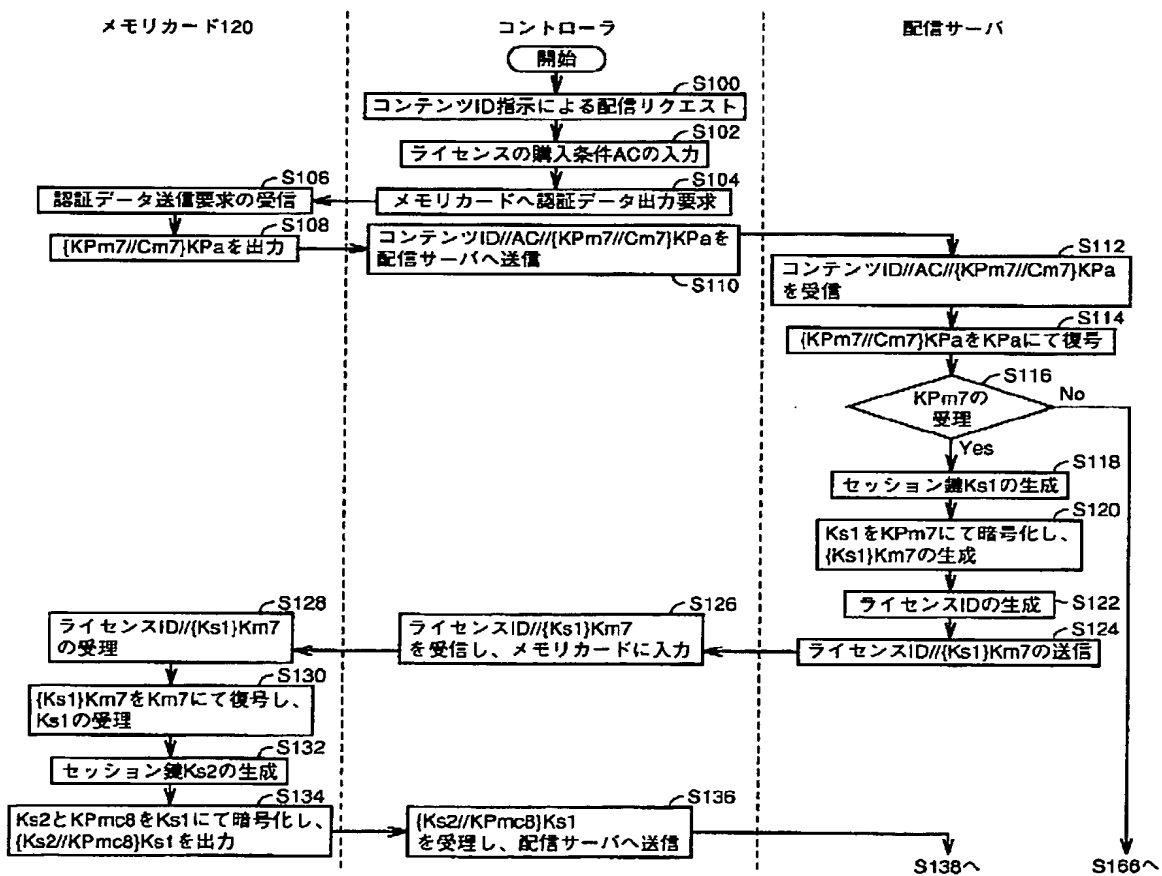
1426



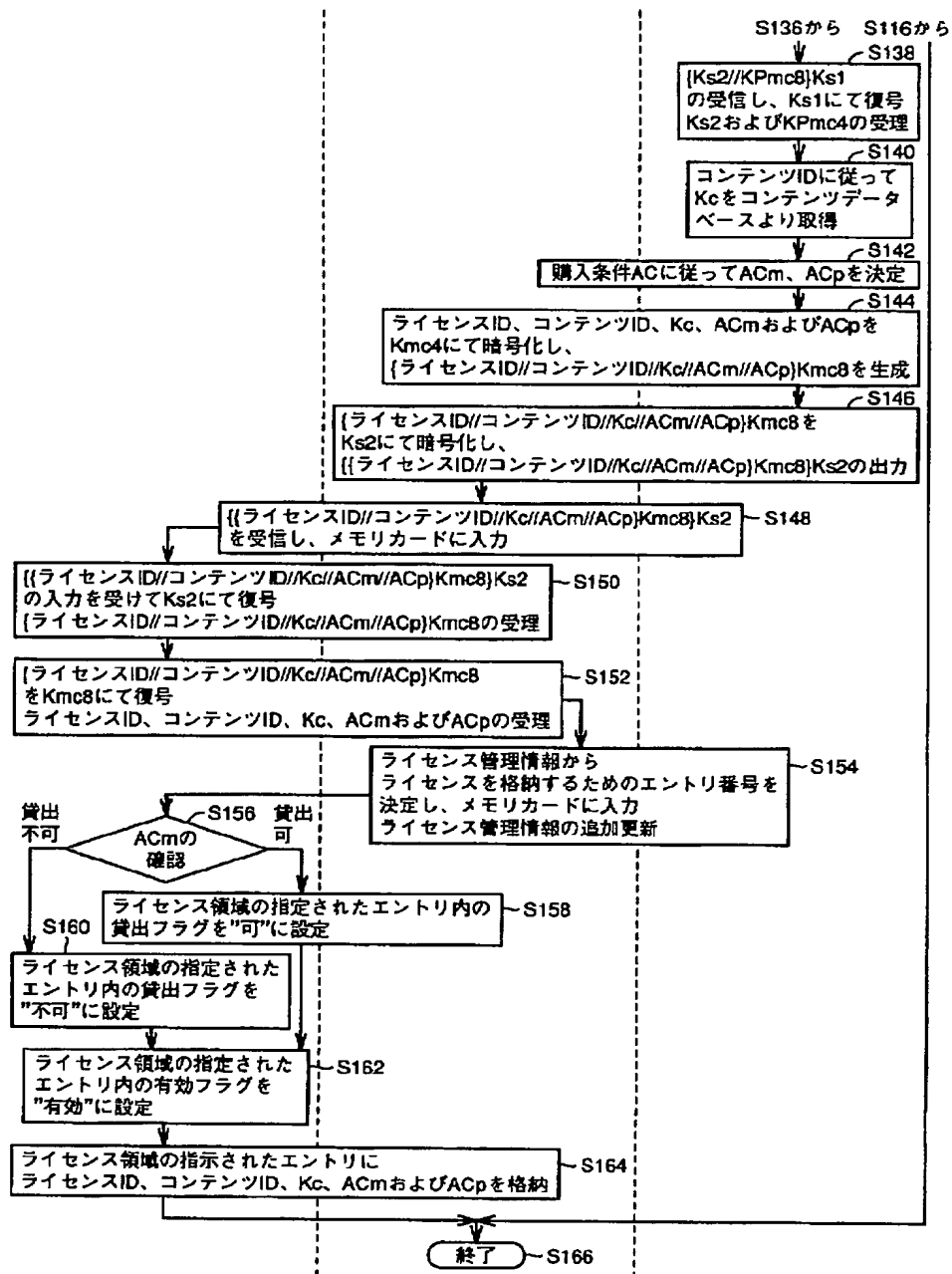
【図9】



【図10】

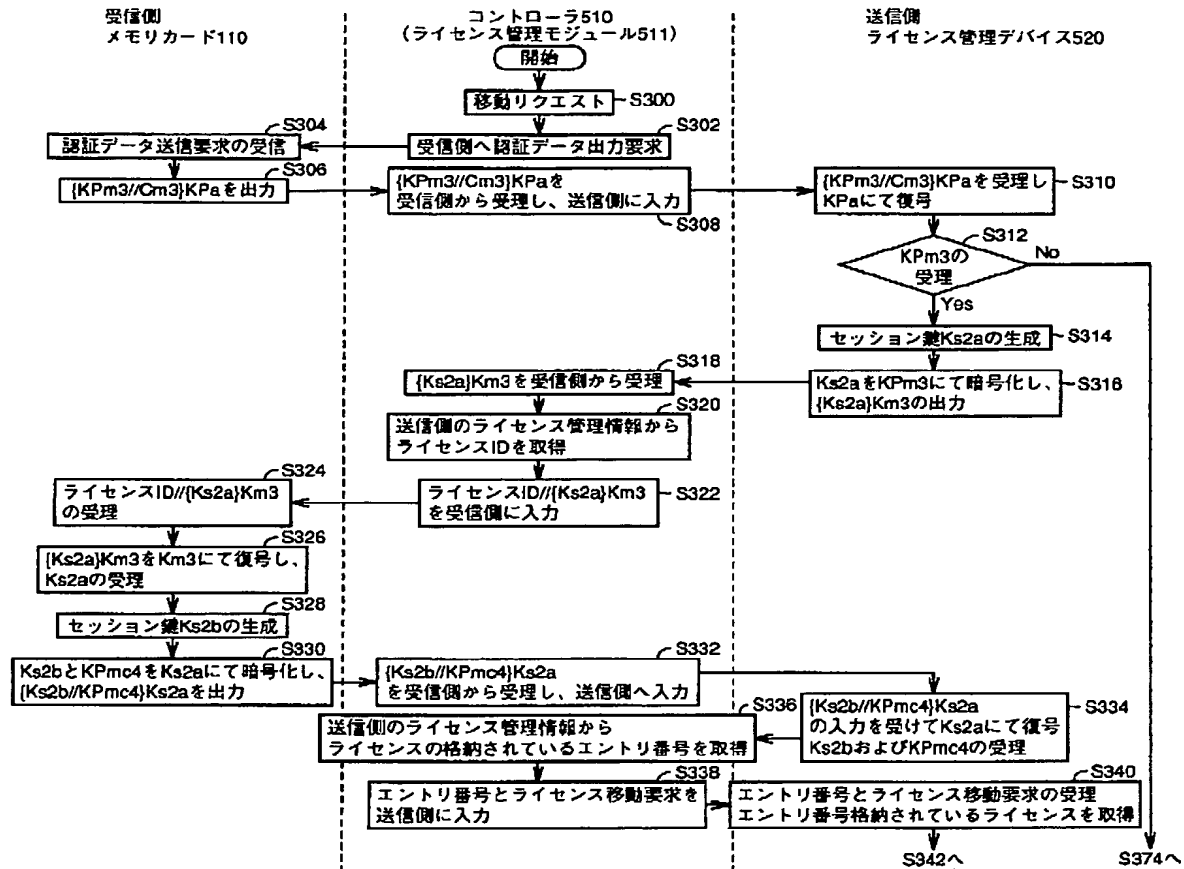


【図11】

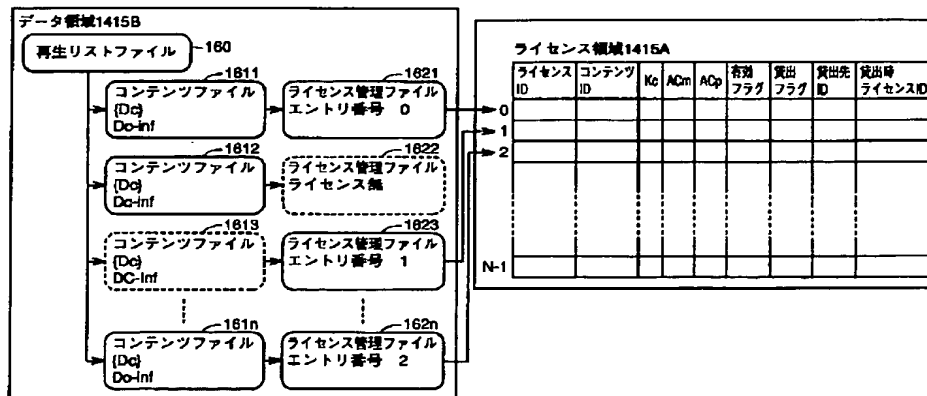




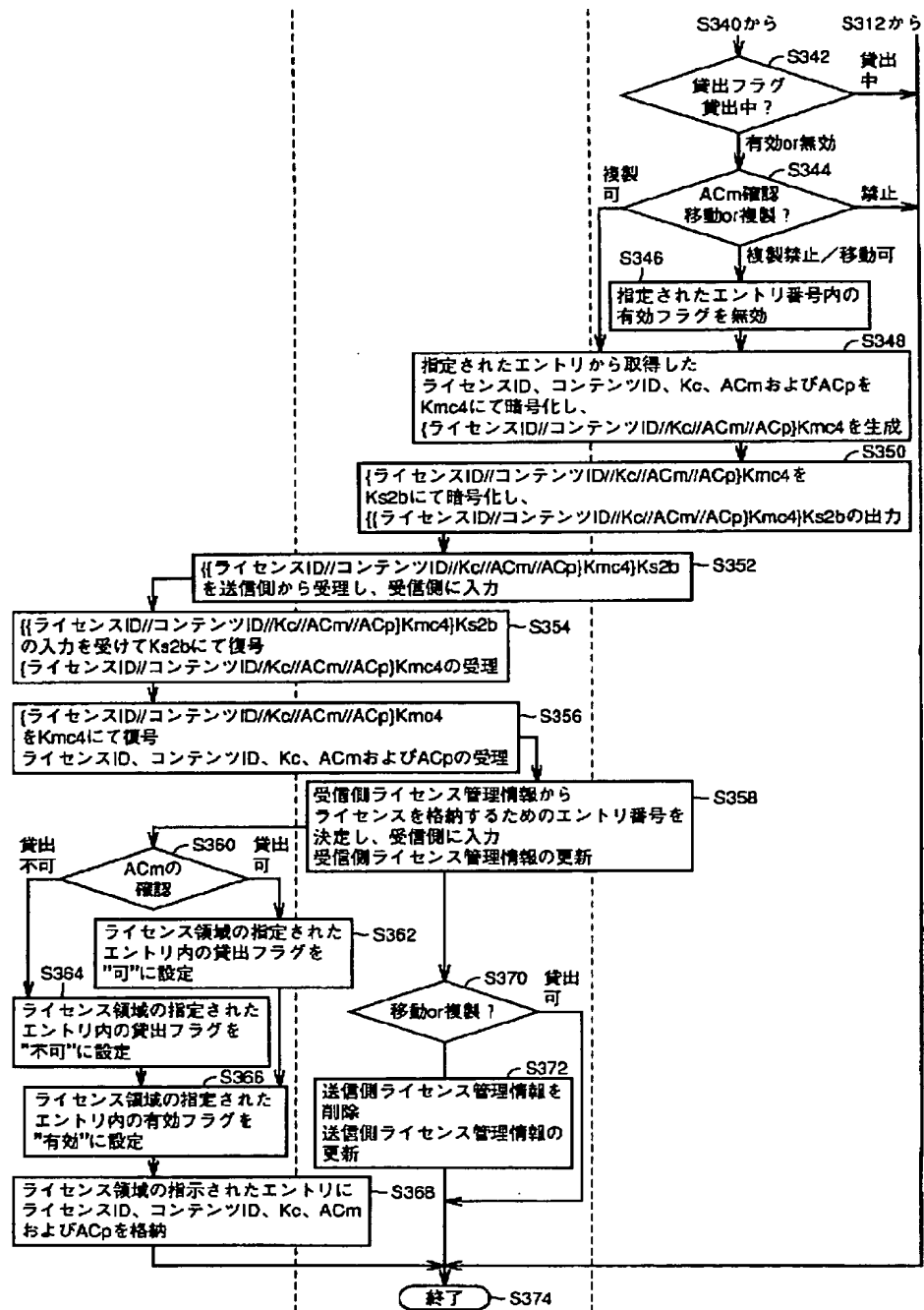
【図14】



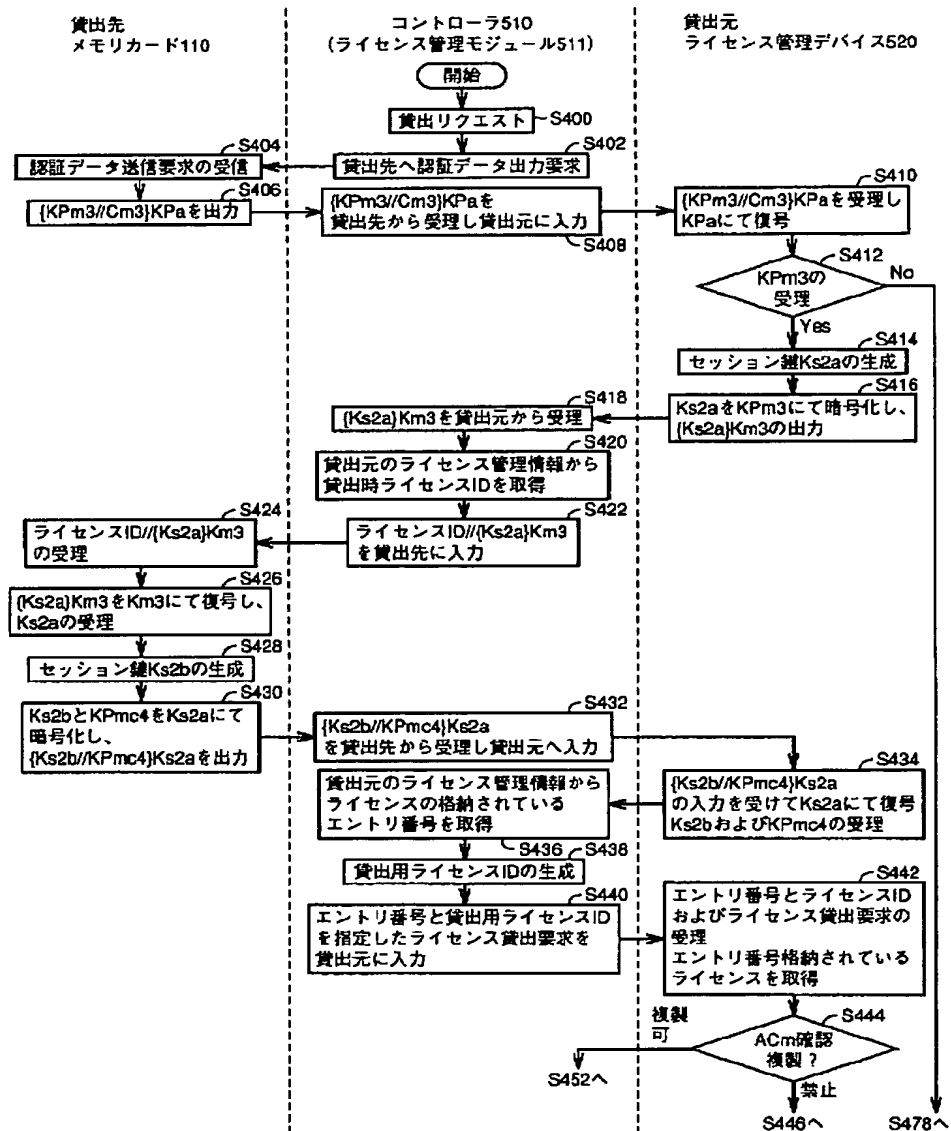
【図23】



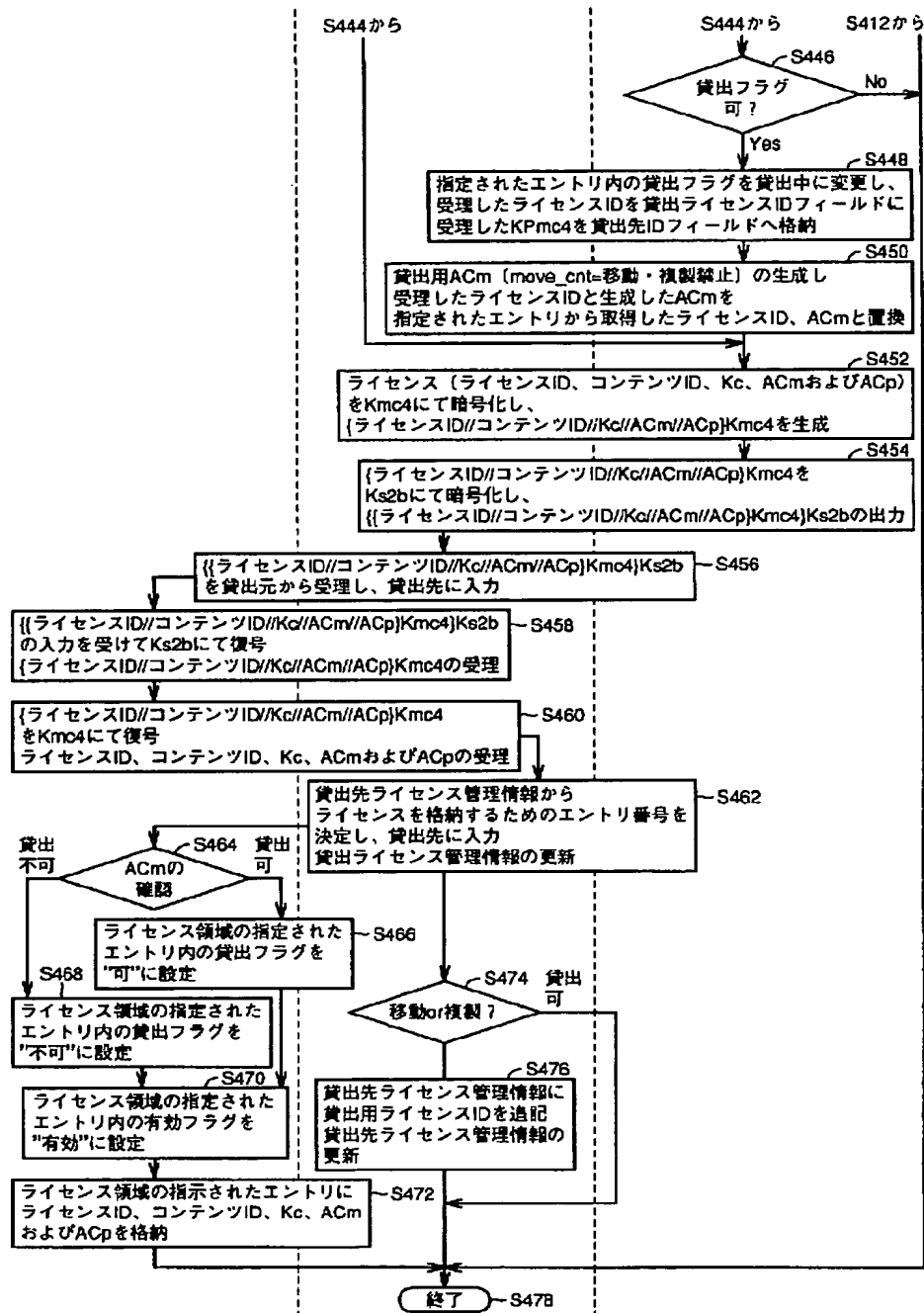
【図15】



【図16】

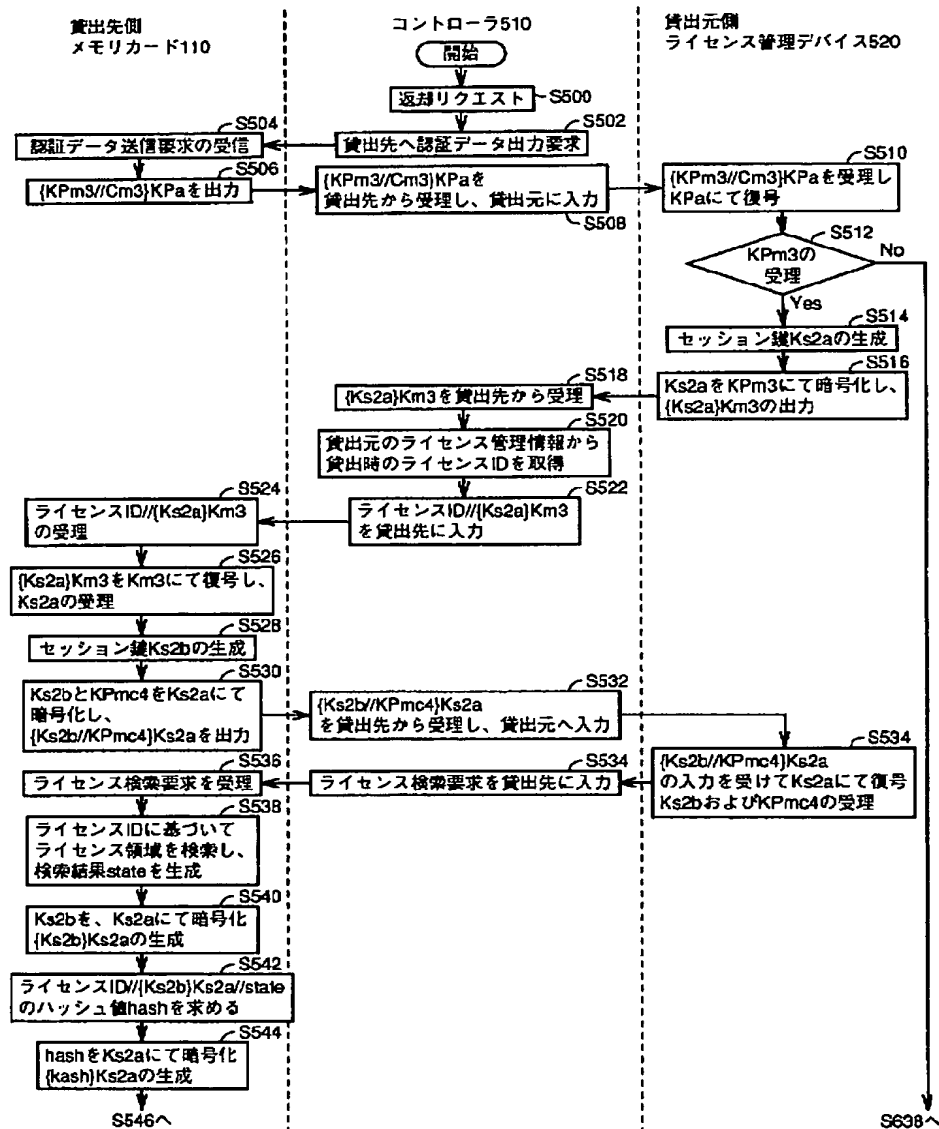


【図17】

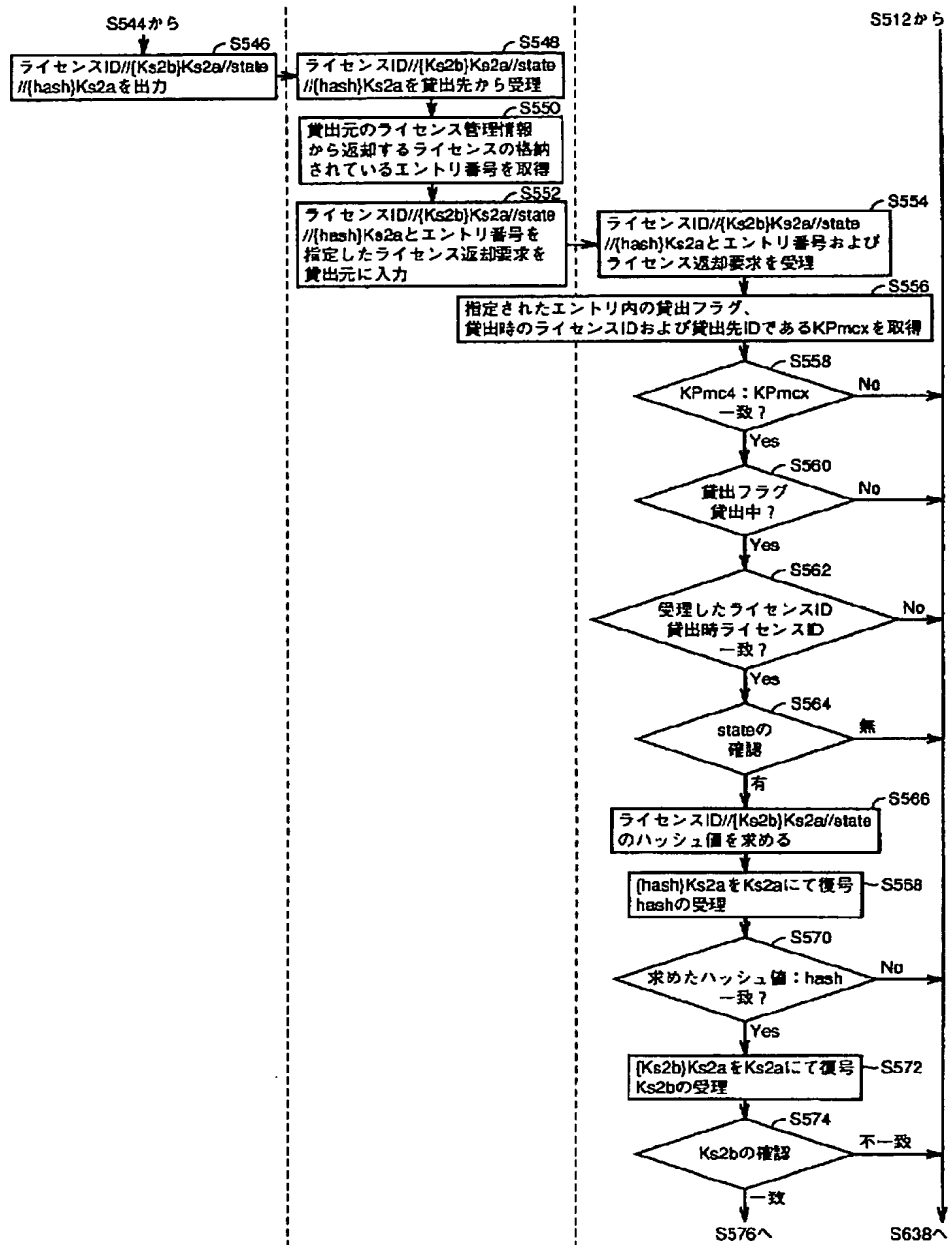




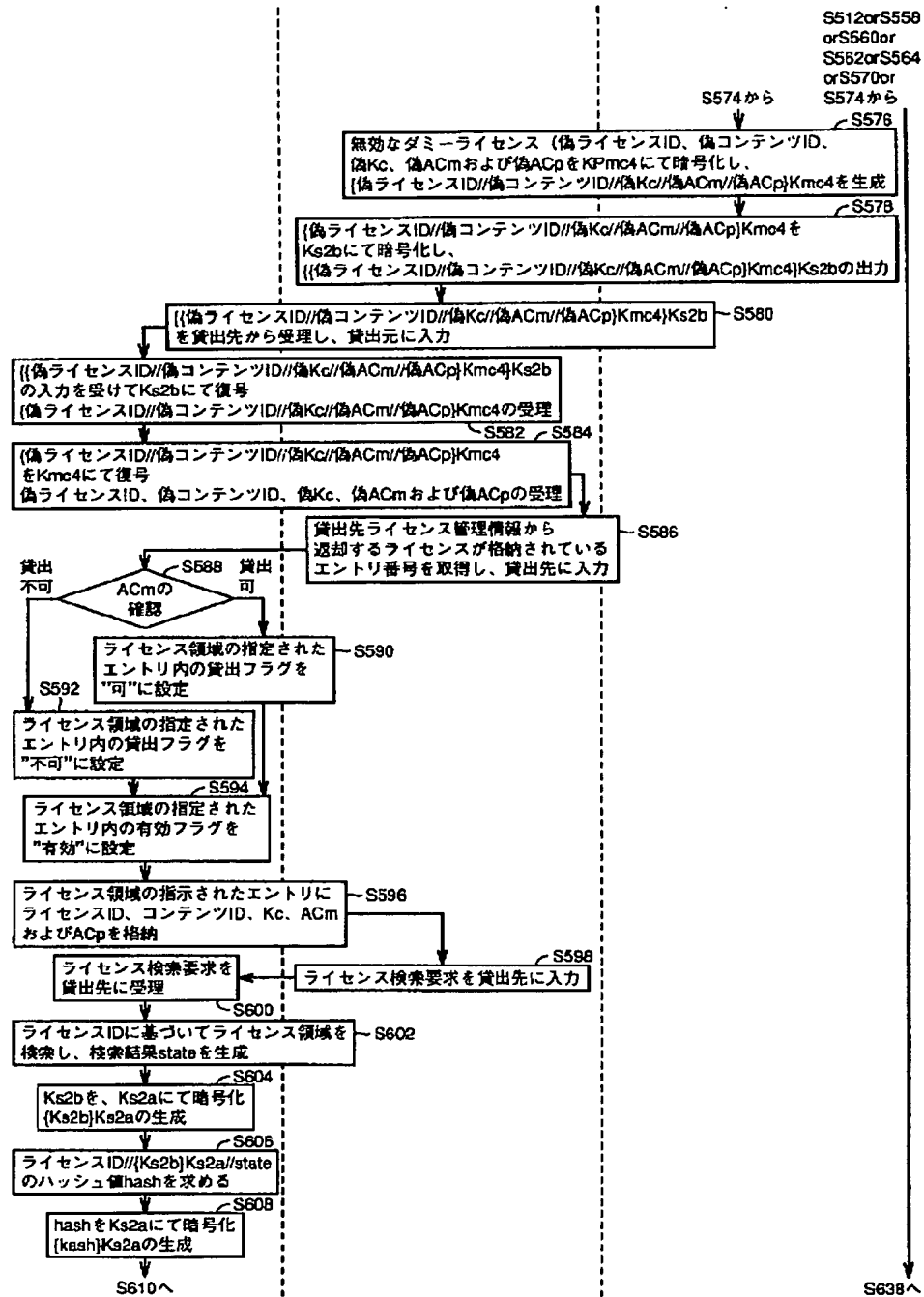
【図18】



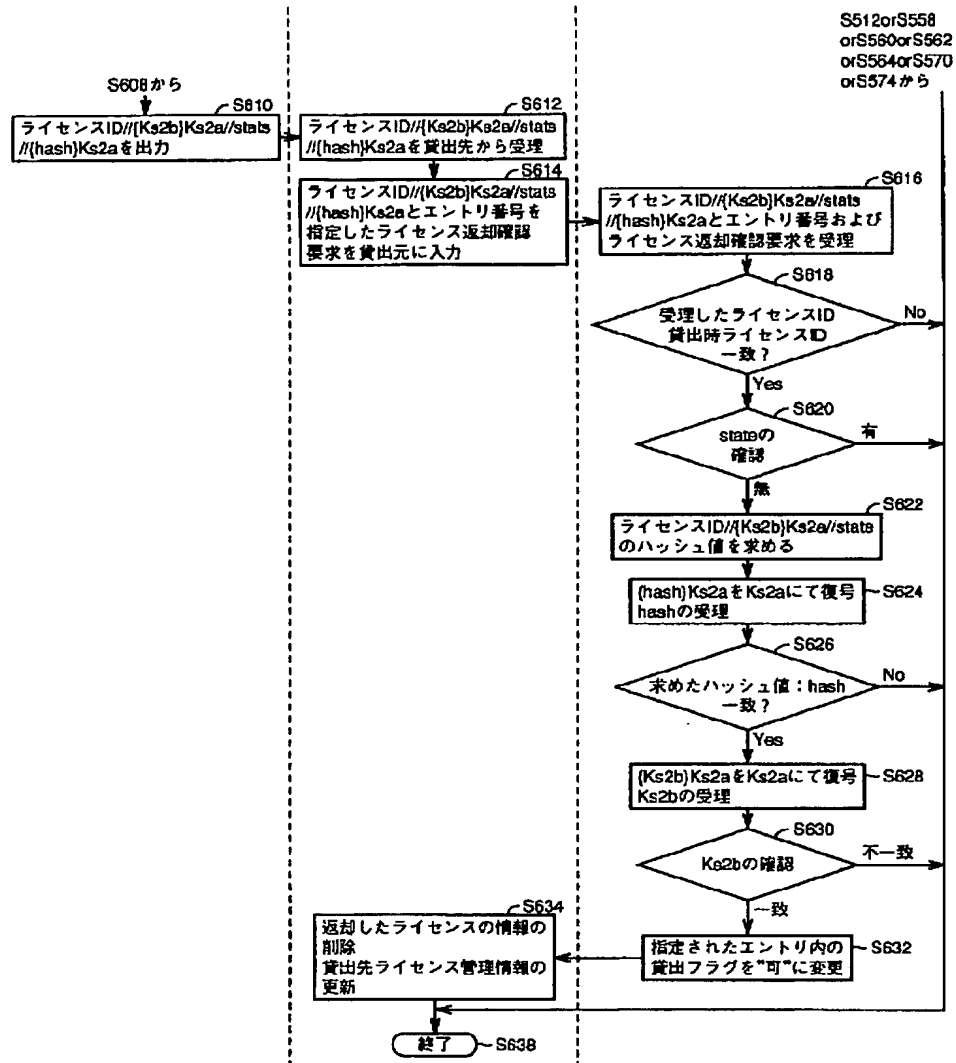
【図19】



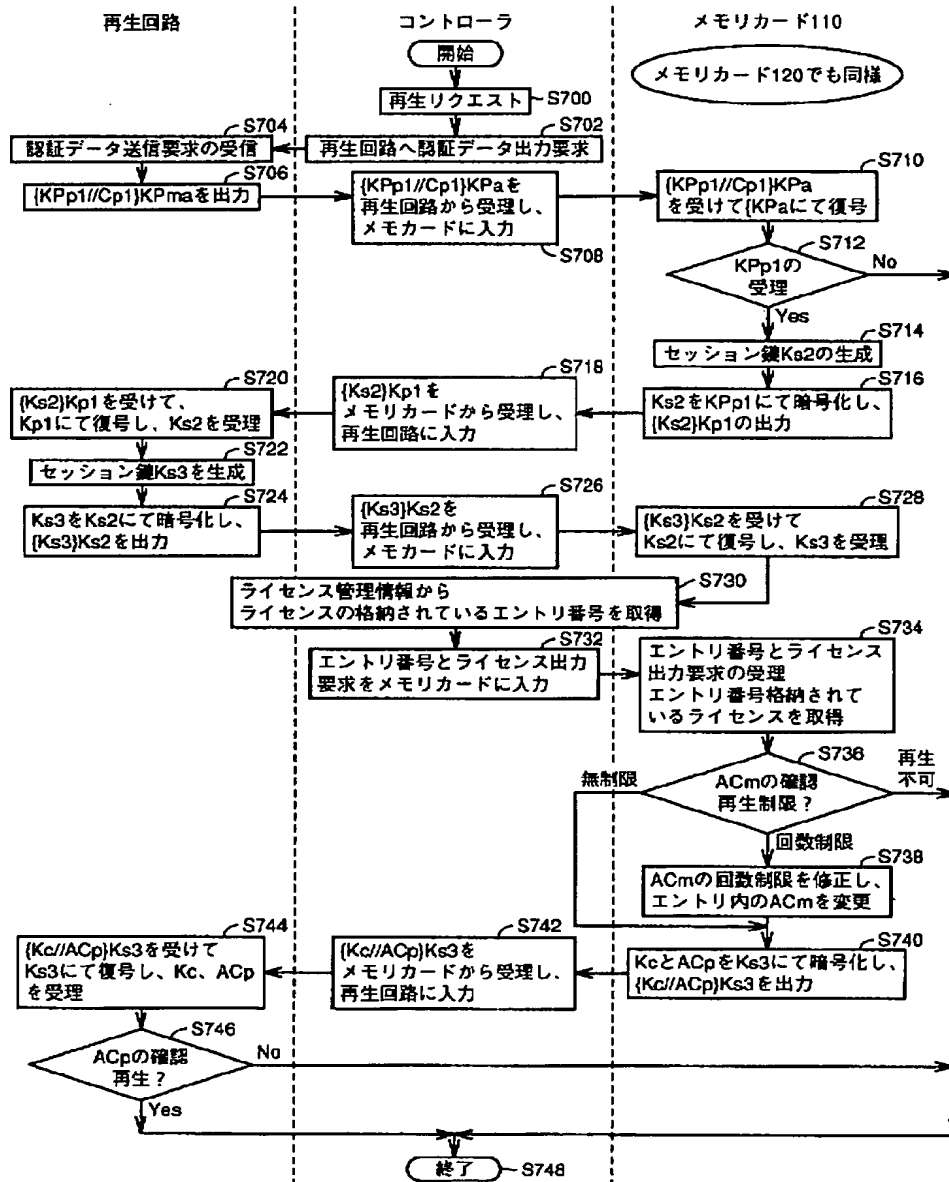
【図20】



【図21】



【図24】



フロントページの続き

(51) Int. Cl.<sup>7</sup>  
G 0 6 K 19/07

識別記号

F I  
G 0 6 K 19/00

テーマコード (参考)  
N